TABLE DES MATIERES

ABREVIATIONS

ACK	:	ACKnowledge character
ACL	:	Access Control List
ARP	:	Address Resolution Protocol
API	:	Application Programming Interface
APT	:	Advanced Package Tool
ATM	:	Asynchronous Transfer Mode
ASCII	:	American Standard Code for Information Interchange
BBS	:	Bulletin Board System
BGP	:	Border Getway Protocol
BOOTP	:	Bootstrap Protocol
BIND	:	Berkeley Internet Name Domain.
CSMA/CD	:	Carrier Sens Multiple Access Code Division
CPU	:	Central Processing Unit
DARPA	:	Defense Advanced Research Projects Agency
DHCP	:	Dynamic Host Configuration Protocol
DMZ	:	De-Militarized Zone
DNS	:	Domaine Name Service
DSL	:	Digital Subscriber Line
FAI	:	Fournisseur d'Accès Internet
FCS	:	Frame Check Sequence
FDDI	:	Fiber Distributed Data Interface
FTP	:	File Transfert Protocol
GGP	:	Getway to Getway Protocol
GNU	:	Gnome Not Unix
HDLC	:	High Data Link Control

HTML	:	HyperText Markup Language
HTTP	:	HyperText Transfert Protocol
ICMP	:	Internet Control Message Protocol
ICP	:	Internet CacheProtocol
IGMP	:	Internet Group Management Protocol
IMAP	:	Internet Message Access Protocol
IP	:	Internet Protocol
Ipfwadm	:	Internet Protocol Firewall administration
IPNG	:	Internet Protocol Next Generation
IPv4	:	Internet Protocol version 4
IPv6	:	Internet Protocol version 6
IPX	:	Internet Packet eXchange
ISO	:	International Standardization Organization
ISP	:	Internet Service Provider
LAN	:	Local Area Network
MAC	:	Medium Access Card
MAN	:	Metropolitan Area Network
MBR	:	Master Boot Record
MX	:	Mail eXchanger
NAT	:	Network Address Translation
NFS	:	Network File System
NIC	:	Network Information Network
NIS	:	Network Information Service
NNTP	:	Network Time Protocol
NTP	:	Network Time Protocol
NVT	:	Network Virtual Terminal
OSI	:	Open System Interconnection

PAR	:	Positive Acknowledgment with Retransmission
POP	:	Post Office Protocol
PUP	:	PARC Universal Memory
PPP	:	Point to Point Protocol
RAM	:	Random Memory Access
RARP	:	Reverse Address Resolution Protocol
RFC	:	Request For Comments
RIP	:	Routing Information Protocol
RPM	:	Red Hat Package Manager
RSS	:	Really Simple Syndication
SGBD	:	Système de Gestion des Bases de Données
SMTP	:	Simple Mail Transfer Protocol
SNMP	:	Simple Network Management Protocol
SSH	:	Secure SHell
SSL	:	Secure Socket Layer
TCP	:	Transfert Control Protocol
TFTP	:	Trivial File Transfer Protocol
TLD	:	Top levels domains
TOS	:	Type Of Service
UDP	:	User Datagram Protocol
UIT-T	:	Union Internationale des Télécommunications
WAIS	:	Wide Area Information Servers
WWW	:	World Wide Web
URL	:	Uniform Resource Locator
XML	:	eXtensible Markup Language

INTRODUCTION

Une entreprise utilise des ordinateurs pour faire du travail. Ces ordinateurs sont souvent connectés entre eux pour faciliter les partages des données, des matériels et logiciels. Un des techniques pour améliorer ce partage, la circulation et les conditions d'utilisation des données est la mise en place d'un réseau intranet dans cette entreprise.

L'intranet est un réseau informatique local et privé propre à une organisation (entreprise, administration ….) qui utilise les techniques de communication d'internet IP mais ne s'ouvre pas aux connexions publiques. L'intranet offre beaucoup d'avantage, de plus il utilise les services de l'Internet mais interne à l'entreprise.

De plus, actuellement, il parait difficile de travailler sans avoir une connexion au réseau internet dans une entreprise. La richesse, la rapidité d'accès, la disponibilité des informations font à internet un outil incontournable, tant pour les entreprises que pour les grands publics. Tout cela montre que l'internet ouvre une autoroute de l'information devant nous. On voit que celle-ci ne permet pas seulement de voyager mais qu'elle permet aussi à un nombre considérable d'étranger de venir chez soi dont certains ne sont pas forcement les bienvenues. C'est pour cette raison qu'on va construire une sorte de pare-feu (Firewall) qui est une forme de protection permettant à un réseau d'être connecté à l'Internet tout en maintenant un certain degré de sécurité.

Pour cela, notre travail se divise en cinq chapitres :

Le premier consiste à une étude théorique comprenant les généralités sur les réseaux. Nous avons pensé qu'il est nécessaire de connaitre ce qui est un réseau, son fonctionnement, ses architectures.

Le second chapitre est intitulé sur le système d'exploitation Linux. L'intranet qu'on va créer fonctionne sous le système d'exploitation Linux pour cela il est nécessaire d'avoir une aperçu concernant ce système d'exploitation.

Le troisième chapitre nous élabore la sécurisation des réseaux. Avant d'entamer l'étude sur le firewall, il est aussi nécessaire de connaitre les types d'attaques, les types d'agresseurs et comment fait-on pour sécuriser les réseaux si on connait ces types d'attaques et ces types d'agresseurs.

Le quatrième chapitre consiste la mise en place de l'intranet dans l'entreprise. Ce chapitre nous explique : comment fait-on pour mettre en place l'intranet, quels sont les outils nécessaires, comment s'effectue le mode de fonctionnement de l'intranet.

Le quatrième chapitre est basé sur l'étude et la mise en ouvre du firewall. Il explique : qu'est ce qu'un firewall, quel est son mode de fonctionnement.

CHAPITRE 1

GENERALITES SUR LES RESEAUX

1.1 Introduction

Avant d'entamer l'étude sur la mise en place de l'intranet et la sécurisation à l'aide d'un firewall, il est nécessaire de connaitre les généralités et les bases sur les réseaux. Ce chapitre nous élabore : les définitions du réseau, les différents types de commutation, les architectures du réseau et les architectures client serveur.

1.2 Définitions d'un réseau

Définitions 1.01

Un réseau est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies.
Un réseau, en général, est le résultat de la connexion de plusieurs machines entre elles, afin que les utilisateurs et les applications fonctionnant puissent échanger des informations. [3]

Le terme réseau, en fonction de son contexte, peut designer plusieurs choses. Il peut designer l'ensemble des machines, infrastructure informatique d'une organisation avec les protocoles qui sont utilisés, ce qui est le cas lorsque l'on parle de l'Internet. [1]

C'est un ensemble d'ordinateurs (ou de périphériques) autonomes connectés entre eux et qui sont situés dans un certain domaine géographique. [3]
Le terme réseau peut également être utilisé pour décrire la façon dont les machines d'un site sont interconnectées .C'est le cas lorsque l'on dit que les machines d'un site sont sur Ethernet, Token Ring, réseau en étoile, réseau en bus,…..

Le terme réseau peut également être utilisé pour spécifier le protocole qui est utilisé pour que les machines communiquent. On peut parler de réseau TCP/IP, Netbeni(protocole Microsoft),Dec Net(protocole DEC),IPX/SPX,…

Le terme réseau possède diffèrent signification, alors à chaque mot réseau il faut comprendre son sens.

Les Réseaux permettent :

- De partager les fichiers.
- Le partage d'application : compilateur, système de gestion de base de données (SGBD).

- Partage d'imprimante.
- L'interaction avec les utilisateurs connectés : messagerie électronique, conférence
- électronique, Talk, ...
- Le transfert de donnée en générale (réseaux informatiques).
- Le transfert de la parole (réseaux téléphoniques).
- Le transfert de la parole, de la vidéo et des données (réseaux à intégration de services ou multimédia). [2]

On compte généralement quatre catégories de réseaux informatiques, différenciées par la distance maximale séparant les points les plus éloignés du réseau. [2]

On distingue :

- Les PAN : Personal Area Network, ces réseaux personnels interconnectent sur quelques mètres les équipements personnels tels que GSM, portables, etc.…[2]
- Les LAN : Local Area Network, correspondent par leur taille aux réseaux intra-entreprises. Ils servent au transport de toutes les informations numériques de l'entreprise. En règle générale, les bâtiments à câbler s'étendent sur plusieurs centaines de mètres. Les débits de ces réseaux vont aujourd'hui de quelques mégabits à plusieurs centaines de mégabits par seconde.[2]
- Les MAN : Metropolitain Area Network, permettent l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit qui est géré à l'échelle d'une métropole. Ils doivent être capables d'interconnecter les réseaux locaux de différentes entreprises pour leur donner la possibilité de dialoguer avec l'extérieur. [2]
- Les WAN : Wide Area Network, sont destinés à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, et il utilise en ce cas des infrastructures au niveau du sol, essentiellement de grands réseaux de fibre optique, soit hertzien, comme les réseaux satellites. [2]

1.3 Différentes techniques de commutation

Le réseau doit permettre l'échange de messages entre les abonnés quelle que soit leur localisation. La commutation rassemble toutes les techniques qui réalisent la mise en relation de deux abonnés quelconques.

Il existe quatre techniques de commutation :

1.3.1 *Commutation de circuits*

Un chemin physique est établi à l'initialisation de la communication entre l'émetteur et le récepteur et reste le même pendant toute la durée de la communication. Si les deux correspondants n'ont pas de données à transmettre pendant un certain temps, la liaison restera inutilisée. L'idée est de concentrer plusieurs correspondants sur une même liaison. Dans le cas où les communications seraient nombreuses, il faut prévoir des mémoires pour stocker des informations en attendant que la liaison soit disponible. [1]

1.3.2 *Commutation de messages*

Un message est un ensemble d'information logique formant un tout (fichier, mail) qui est envoyé de l'émetteur vers le récepteur en transitant nœud à nœud à travers le réseau. On a un chemin logique par message envoyé. Le message ne peut être envoyé au nœud suivant tant qu'il n'est pas reçu complètement et sans erreur par le nœud actuel. [3]

Remarque : La commutation de message nécessite la mise en place d'algorithmes de routage.

1.3.3 *Commutation de paquets*

Optimisation de la commutation de message qui consiste à découper les messages en plusieurs paquets pouvant être acheminés plus vite et indépendamment les uns des autres. Cette technique nécessite la mise en place de la numérotation des paquets. [1]

1.3.4 *Commutation de cellule*

Commutation de paquets particulière. Tous les paquets ont une longueur fixe de 53 octets (1 paquet = 1 cellule de 53 octets).C'est la technique utilisée dans les réseaux ATM où un chemin est déterminé pour la transmission des cellules. [1]

Commutation de cellule = superposition de deux types de commutation :

- commutation de circuit
- commutation de paquets. Il utilise le mode connecté

- Mode connecté : Demande explicite de connexion et de déconnexion.
- Mode non connecté : Pas de demande de connexion.

1.4 Architecture des réseaux

Pour assurer le bon transfert de l'information avec une quantité de service suffisante, il faut prévoir une architecture logicielle. Une normalisation de l'architecture logicielle s'impose.

Deux grandes familles d'architecture se disputent dans le marché. La première provient de l'ISO. L'OSI. La deuxième est TCP/IP. Une troisième est celui de l'UIT-T, il s'agit de l'adaptation du modèle OSI pour prendre en compte les réseaux hauts-débit (réseau ATM).

1.4.1 *Modèle de référence OSI*

Le modèle de référence OSI publié en 1984 fut le modèle descriptif de réseau créé par l'ISO. Ce modèle propose aux fournisseurs un ensemble de normes assurant une compatibilité et une interopérabilité accrues entre divers types de technologies réseau produites par de nombreuses entreprises à travers le monde.

Elle comporte sept couches numérotées, chacune illustrant une fonction réseau bien précise. Cette répartition des fonctions réseau est appelée organisation en couches. Le découpage du réseau en sept couches présente les avantages suivants :

- Il permet de diviser les communications sur le réseau en éléments plus petits et plus simples.
- Il uniformise les éléments du réseau afin de permettre le développement et le soutien multi-constructeur. [4]
- Il permet à différents types de matériel et de logiciel réseau de communiquer entre eux.
- Il empêche les changements apportés à une couche d'affecter les autres couches, ce qui assure un développement plus rapide. [4]
- Il divise les communications sur le réseau en éléments plus petits, ce qui permet de les comprendre plus facilement.

La figure suivante représente le modèle sept couches d'OSI

Figure 1.01 : *Couches fonctionnelles du modèle OSI*

Cette figure permet de voir que les protocoles forment un empilement de blocs de constructions posés les uns sur les autres. C'est en cette raison de cette apparence que la structure est souvent appelée une pile (stack) ou pile de protocoles.

Pour permettre l'acheminement des données entre l'ordinateur source et l'ordinateur de destination, chaque couche possède sa propre fonction et la couche au niveau de l'ordinateur source doit communiquer avec sa couche homologue sur l'ordinateur de destination, chaque couche dépend de la fonction de service de la couche sous-jacente. [4] [5]

Examinons les fonctions de chaque couche

- La couche physique :

Elle détermine la caractéristique des matériels à utiliser pour la liaison physique entre équipement d'un réseau (câble, connecteur, concentrateur, commutateur). Elle a en charge la transmission des suites des bits sur les moyens physiques d'interconnexion mais aussi le traitement de signal (modulation, amplification, …). [4] [6]

- La couche liaison des données :

La couche liaison détermine la technique d'accès au media qui varie en fonction du type de réseau (Ethernet ou Token-Ring). Elle assure le transfert fiable de données par le média c'est-à-dire sans erreurs, sans duplication ni perte entre systèmes adjacentes (donc sur un seul circuit de données), l'adressage physique, notification des erreurs, contrôle de flux. [4]

- La couche réseau :

La couche réseau a pour rôle de gérer, d'établir et de maintenir les connexions de réseau entre deux systèmes d'extrémité et la sélection du meilleur chemin possible, c'est-à-dire l'adressage logique et le routage. Par ailleurs elle se charge des moyens fonctionnels et les procédures nécessaires pour échanger, entre les entités de transport, des unités du service de réseau. [4]

- La couche transport :

Cette couche assure la connexion bout à bout des informations du réseau, transport des données entre les hôtes. Elle établisse l'ouverture et la fermeture des circuits virtuels, détecte les pannes et reprise des erreurs, gère le contrôle de flux. [4]

- La couche session:

La couche session ouvre, gère et ferme les sessions entre les applications. Cela comprend le lancement, l'arrêt et la resynchronisation de deux ordinateurs qui communiquent. Elle coordonne les applications lorsqu'elles interagissent sur deux hôtes qui communiquent. [4]

- La couche présentation :

Cette couche assure la lisibilité des données pour le système de destination, indique le format des données, structure les données. Elle négocie la syntaxe de transfert des données pour les applications.

- La couche application :

Cette couche fournit les services de communication aux utilisateurs (opérateurs, périphériques, programme d'application). Elle fourni également des services réseaux aux processus d'applications (courrier électronique, transfert des fichiers et émulations des terminal). [4]

1.4.2 *Architecture du modèle TCP-IP*

La pile de protocoles TCP/IP a été développée dans le cadre des recherches de la DARPA. Elle était initialement destinée à assurer les communications au sein de la DARPA. Ensuite, elle a été intégrée à la distribution Berkeley du système d'exploitation Unix. Aujourd'hui, la suite de protocoles TCP/IP est devenue la norme des communications inter-réseaux et sert de protocole de transport à Internet, ce qui permet à des millions d'ordinateurs de communiquer entre eux. [4]

L'architecture TCP/IP prend comme modèle de référence le modèle OSI, mais avec seulement quatre couches fonctionnels : la couche application, la couche transport, la couche Internet et la

couche d'accès au réseau. Autrement dit, certaines couches du modèle TCP/IP portent le même nom que des couches du modèle OSI. Il ne faut pas confondre les couches des deux modèles, car la couche application comporte des fonctions différentes dans chaque modèle. La figure suivante permet de visualiser ces quatre couches du modèle TCP/IP.

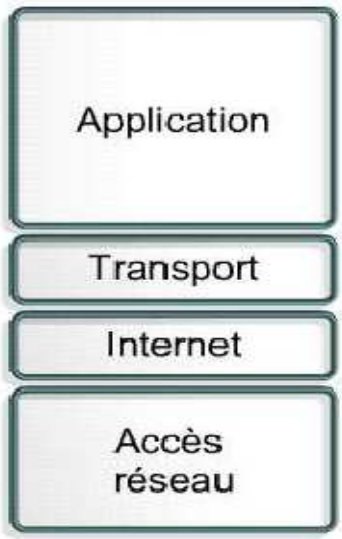

Figure 1.02 : *Couches fonctionnelles du modèle TCP-IP*

Le terme TCP/IP est un ensemble de protocole qui permet au réseau d'échanger des informations. Ces protocoles assurent la bonne circulation des flux à travers le réseau.

De même que pour le modèle OSI, les données sont passées vers le bas de la pile quand elles sont envoyées vers le réseau, et vers le haut quand elles sont reçues. La structure à quatre niveaux de TCP-IP est vue de la façon dont les données sont gérées alors qu'elles traversent la pile de protocoles vers le réseau physique. Chacune des couches de la pile ajoute des informations de contrôle afin d'assurer une livraison correcte .Ces informations de contrôle sont appelées un en-tête parce qu'elles sont placées devant les données à transmettre. Chaque couche traite toutes les informations qu'elle reçoit des couches supérieures en tant que données et place son propre en-tête avant elles. L'addition d'informations de distribution à chaque couche est appelée encapsulation.

Quand les données sont reçues, c'est l'inverse qui se produit. Chaque couche enlève son en-tête avant de passer les données à celle du dessus. Les informations reçues d'une couche sont interprétées en tant qu'en-tête et données. [1] [2] [4]

Illustrons à l'aide d'une figure l'encapsulation des données (respectivement la désencapsulation) et les protocoles utilisés

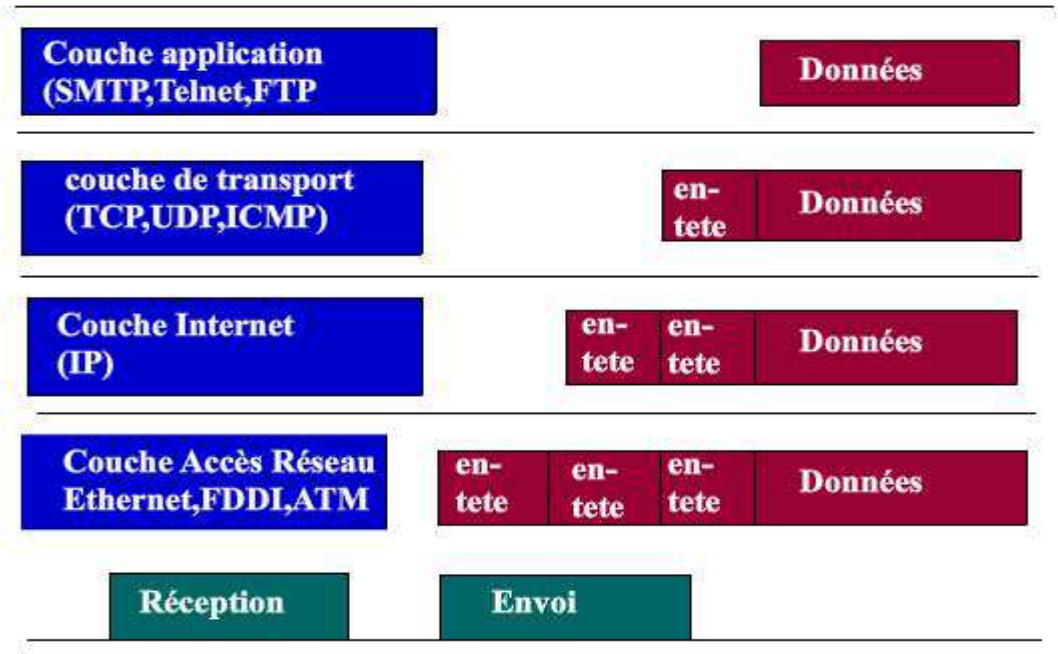

Figure 1.03 *: Encapsulation des données*

Examinons plus attentivement la fonction de chaque couche :

1.4.2.1 Couche d'Accès Réseau

La couche d'Accès Réseau est le plus bas niveau de la hiérarchie des protocoles TCP/IP. Les protocoles de cette couche fournissent le moyen de délivrer des données aux autres systèmes directement rattachés au réseau. Il définit la façon d'utiliser le réseau pour transmettre un datagramme IP. [4] [5]

La couche d'Accès Réseau doit connaitre les détails du réseau sous-jacent (sa structure de paquets, son adressage, etc.)Pour formater correctement les données transmises afin de se conformer aux contraintes du réseau. La couche d'Accès Réseau TCP/IP peut regrouper les fonctions des trois couches les plus basses du modèle OSI (Réseau, Liaison et Physique).

Les fonctions assurées à ce niveau comprennent l'encapsulation des datagrammes IP dans les trames transmises par le réseau et la correspondance des adresses IP vers les adresses physiques utilisées par le réseau.

1.4.2.2 Couche Internet

La couche située au-dessus de la couche d'Accès Réseau dans la hiérarchie des protocoles est la couche Internet. Le protocole Internet (IP), est au cœur de TCP/IP et le protocole le plus important de la couche Internet. IP fournit les services de livraison de paquets de base sur lesquels les réseaux TCP/IP sont construits. Tous les protocoles des couches supérieures (TCP, UDP) et inferieures (Ethernet, FDDI, ATM, etc..) utilisent IP pour délivrer les données. Toutes les données TCP/IP passent par IP, qu'elles soient entrantes ou sortantes quelque soit sa destination finale. [5]

Les fonctions d'IP sont :

- La définition du datagramme, qui est l'unité de base de transmission de l'internet
- La définition du principe d'adressage de l'Internet
- Le passage des données entre la couche d'Accès Réseau et la couche transport Hôte à Hôte
- Le routage des datagrammes vers les machines distantes
- La fragmentation et le réassemblage des datagrammes

Les données qui franchissent la couche IP, alias couche Internet, sont appelées " datagramme IP ", datagramme Internet ou datagramme tout court. Voyons les caractéristiques de ces datagrammes

1.4.2.2.1 Les datagrammes

Les données circulent sur l'Internet sous forme des datagrammes ou des paquets. Les datagrammes sont des données encapsulées, c'est-à-dire des données auxquelles on a ajouté des en-têtes correspondant à des informations sur leur transport ; telles que l'adresse IP destination, adresse IP source, etc.

Les données contenues dans les datagrammes sont analysées et éventuellement modifiées par les routeurs permettant leur transit.

Voici ce en quoi ressemble un datagramme

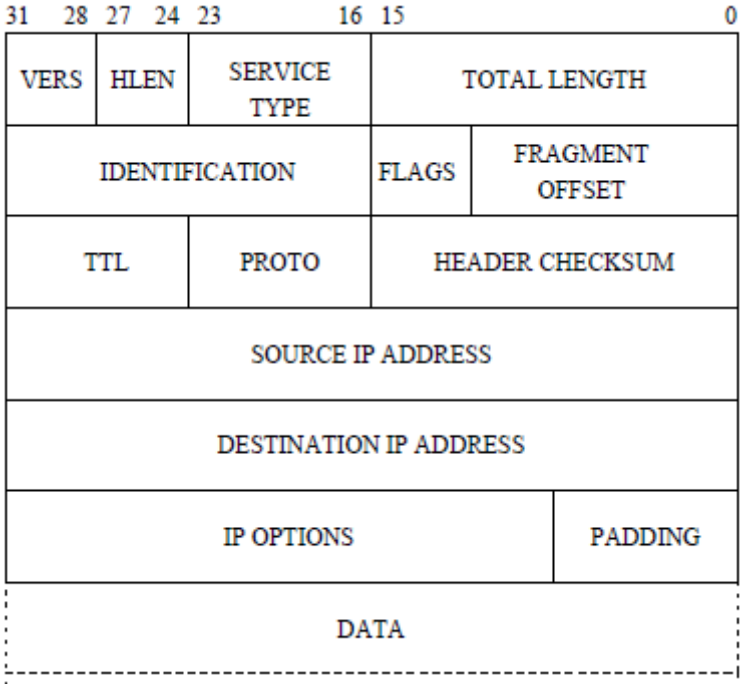

Figure 1.04 : *Format d'un datagramme*

Signification des différents champs

- VERS (Version) : 4 bits qui spécifient la version du protocole IP. L'objet de ce champ est la vérification que l'´emetteur et le destinataire des datagrammes sont bien en phases avec la même version. Actuellement c'est la version 4 qui est principalement utilisé sur l'Internet, bien que quelques implémentations de la version 6 existent et soient déjà en expérimentation. [5]
- HLEN (Longueur d'en-tête) :4bits qui donnent la longueur de l'en-tête en mots de 4 octets ou 32bits. La taille standard de cet en-tête fait 5 mots, la taille maximale fait :$(2^3 + 2^2 + 2^1 + 2^0) \times 4 = 60$ octets. [1] [8]
- SERVICE TYPE (Type de service) : 8bits (4utiles), il indique la façon dont le datagramme doit être traité Suivant les valeurs de ce champ, le routeur peut privilégier un datagramme par rapport à un autre. [1] [8]
- TOTAL LENGHT (Longueur totale) : Il indique la taille totale du datagramme en octets. La taille de ce champ étant de 2 octets, la taille totale du datagramme ne peut dépasser 65536 octets. Utilisé conjointement avec la taille de l' en-tête, ce champ permet de déterminer où sont situées les données. [8]
- IDENTIFICATION, FLAGS et FRAGMENT OFFSET (Identification, drapeau, déplacement de fragment) Ces mots sont prévus pour contrôler la fragmentation des datagrammes. Les données sont fragmentées car les datagrammes peuvent avoir à

traverser des réseaux avec des supports physiques (MTU) plus petits que celui du premier support physique employé. [8]

- TTL “ Time To Live ” 8 bits, 255 secondes maximum de temps de vie pour un datagramme sur le réseau. Prévu a l’origine pour décompter un temps, ce champ n’est qu’un compteur décrémenté d’une unité a chaque passage du datagramme dans un routeur. Couramment la valeur de départ est 32 ou même 64. Son objet est d’´eviter la présence de paquets fantômes circulant indéfiniment. Si un routeur passe le compteur à zéro avant délivrance du datagramme, un message d’erreur est renvoyé à l’émetteur avec l’indication du routeur, le paquet en lui-même est perdu [8]
- PROTO(Protocole) 8 bits pour identifier le format et le contenu des données. Ce champ permet de savoir de quel protocole est issu le datagramme, soit :
  ICMP, IGMP, TCP, UDP
- HEADER CHECKSUM (Somme de contrôle de l’en-tête) : codée sur 16 bits permet de contrôler l’intégrité de l’en-tête afin de déterminer si celui-ci n’a pas été modifié, altéré pendant la transmission. [8]
- SOURCE ADDRESS (Adresse IP source) : ce champ représente l’adresse IP de la machine émettrice, il permet au destinataire de répondre
- DESTINATION IP ADDRESS (Adresse IP destination) : Adresse IP du destinataire du datagramme.
- IP OPTIONS : 24 bits pour préciser des options de comportement des couches IP traversées et destinatrices. Les options les plus courantes concernent :
  – Des problèmes de sécurité
  – Des enregistrements de routes
  – Des enregistrements d’heure
  – Des spécifications de route à suivre
- PADDING Remplissage pour aligner sur 32 bits.
- DATA : les données

1.4.2.3 Couche Transport

La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. Les protocoles de transport définissent comment transmettre les messages entre les hôtes. Les deux protocoles de transport les plus courants sont le protocole TCP et le protocole UDP. Le protocole IP utilise ces protocoles de transport pour permettre aux hôtes de communiquer et de transmettre des données. [8]

1.4.2.3.1 *User Datagram Protocol (UDP)*

L'User Datagram Protocol donne aux programmes d'application un accès direct à un service de transmission de datagrammes, comme celui que fournit IP. Les applications peuvent ainsi échanger des messages sur le réseau avec un minimum de surcharge due au protocole. UDP est un système d'acheminement « au mieux » qui ne nécessite pas d'accusé de réception. UDP est à préférer, notamment pour la lecture audio en continu, la vidéo et la voix sur IP (VoIP). Les accusés de réception ralentiraient la livraison, et les retransmissions ne sont pas souhaitables. [1] [8]

Voici le format du message UDP :

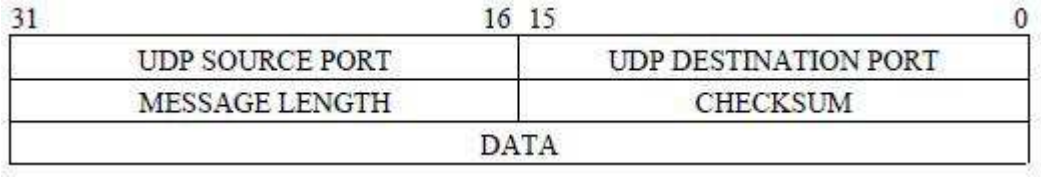

Figure 1.05 : *Format de message UDP*

- UDP SOURCE PORT Le numéro de port de l'´emetteur du paquet. Ce champ est optionnel, quand il est spécifie il indique le numéro de port que le destinataire doit employer pour sa réponse. La valeur zéro indique qu'il est inutilisé, le port 0 n'est donc pas celui d'un service valide. [8]
- UDP DESTINATION PORT Le numéro de port du destinataire du paquet.
- MESSAGE LENGTH C'est la longueur du paquet, donc comprenant l'en-tête
- et le message.
  - La longueur minimale est 8
  - La longueur maximale est 65 535 − *H*(*IP*).
- CHECKSUM Le checksum est optionnel et toutes les implémentations ne l'utilisent pas. S'il est employé, il porte sur un pseudo en-tête, Ce pseudo en-tête est prévu initialement pour apporter une protection en cas de datagrammes mal routés. [1] [8]
- DATA : les données

1.4.2.3.2 *Transmission Control Protocol (TCP)*

Une application qui a besoin d'un accusé de réception, pour s'assurer que le message est bien transmis, utilise TCP. TCP découpe un message en petits morceaux appelés segments. Les segments, numérotés en séquence, sont ensuite passés au processus IP pour être assemblés en paquets. TCP conserve une trace du nombre de segments qui ont été envoyés à un hôte donné à partir d'une application spécifique. Si l'expéditeur ne reçoit pas d'accusé de réception au bout

d'un certain temps, il suppose que les segments ont été perdus, et il les retransmet. Seule la partie du message qui a été perdue est renvoyée, pas l'intégralité. Sur l'hôte récepteur, TCP est responsable de la reconstitution des segments de message et de leur transmission à l'application.TCP est orienté connexion. Il établit une connexion logique de bout en bout entre les deux hôtes communiquant entre eux.

Voici un format de segment TCP

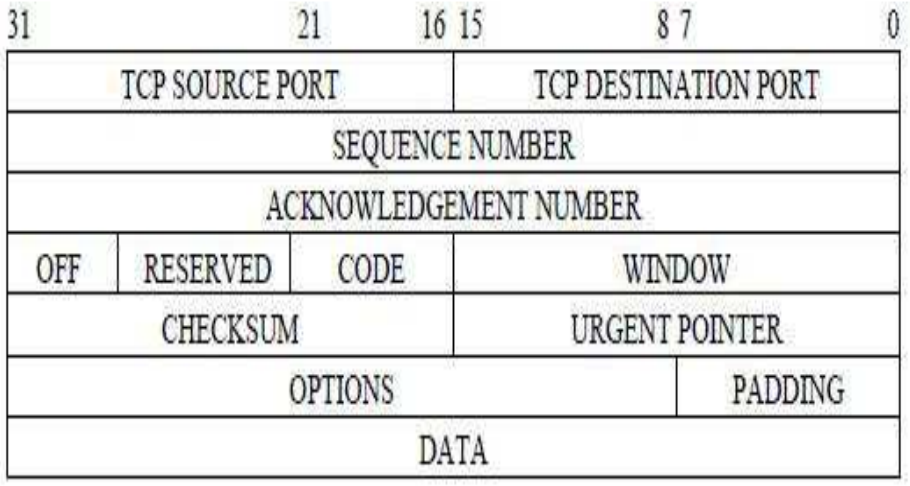

Figure 1.06 : *Format d'un segment TCP*

- TCP SOURCE PORT Le numéro de port de l'application locale.
- TCP DESTINATION PORT Le numéro de port de l'application distante.
- SEQUENCE NUMBER C'est un nombre qui identifie la position des données à transmettre par rapport au segment original
- ACKNOWLEDGEMENT NUMBER C'est un numéro qui identifie la position du dernier
- octet reçu dans le flux entrant.
- OFF pour OFFSET, il s'agit d'un déplacement qui permet d'atteindre les données quand il y a des options. Codé sur 4 bits, il s'agit du nombre de mots de 4 octets qui composent l'en-tête. RESERVED Six bits réserves pour un usage futur
- CODE Six bits pour influer sur le comportement de TCP en caractérisant l'usage du segment
- WINDOW Le flux TCP est contrôlé de part et d'autre pour les octets compris dans une zone bien délimitée et nommée " fenêtre ". La taille de celle-ci est définie par un entier non signé de 16 bits, qui en limite donc théoriquement la taille à 65 535 octets
- CHECKSUM Un calcul qui porte sur la totalité du segment, en-tête et données
- URGENT POINTER Ce champ n'est valide que si le drapeau URG est armé
- OPTIONS C'est un paramétrage de TCP. Sa présence est détectée d`es lors que l'OFFSET est supérieur à 5.

- PADDING Remplissage pour se caler sur un mot de 32 bits.
- DATAS Les données transportées. Cette partie est de longueur nulle à l'´etablissement de la connexion. [8]

1.4.2.4 Couche Application

La couche application se trouve au sommet de l'architecture des protocoles TCP/IP. Cette couche comprend tous les processus qui emploient les protocoles de la couche transport pour délivrer les données. Ils existent de nombreux protocoles d'application. Les plus connues sont :

- FTP : ce protocole est un service fiable orienté connexion qui utilise le protocole TCP pour transférer des fichiers entre des systèmes qui le prennent en charge. Il gère les transferts bidirectionnels des fichiers
- TFTP : ce protocole est un service non orienté connexion qui utilise le protocole de datagramme utilisateur UDP .Il est utilisé sur le routeur pour transférer des fichiers de configuration et des images de la plate-forme logicielle, ainsi que pour transférer des fichiers entre des systèmes qui le prennent en charge. Il est utile dans certains LAN, car il s'exécute plus rapidement que le protocole FTP dans un environnement stable.
- SMTP : ce protocole régit la transmission du courrier électronique sur les réseaux informatiques. Il ne permet pas de transmettre des données autres que du texte en clair.
- DNS: ce protocole est utilisé par Internet pour convertir en adresses IP les noms de domaine et leurs nœuds de réseau annoncés publiquement.
- Telnet : ce protocole permet d'accéder à distance à un autre ordinateur. Cela permet à un utilisateur d'ouvrir une session sur un hôte Internet et d'exécuter diverses commandes. Un client Telnet est qualifié d'hôte local. Un serveur Telnet est qualifié d'hôte distant.
- RIP : employé par des périphériques réseau pour échanger des informations de routages
- NFS: ce protocole est un ensemble de protocoles pour systèmes de fichiers distribués, développé par Sun Microsystems, permettant un accès aux fichiers d'un équipement de stockage distant, tel qu'un disque dur, dans un réseau. [1] [2] [8]
- SNMP : ce protocole permet de surveiller et de contrôler les équipements du réseau, ainsi que de gérer les configurations, les statistiques, les performances et la sécurité. [8]

TCP/IP emploie trios principe pour parvenir à délivrer les données entre deux hôtes:

- L'adressage
- Le routage
- Le multiplexage

1.4.2.4.1 *L'adressage*

L'adressage consiste à affecter une adresse IP sur l'hôte. Les adresses IP sont divisées en groupes de 8 bits séparées par des points, et représentées dans un format décimal. Une adresse IP contient une partie réseau et une partie hôte. On distingue cinq classes d'adresse :

La classe A et B : réservée pour des applications de trafic très élevé

La classe C : utilisé pour les réseaux privés

La classe D : pour l'application multidiffusion

La classe E : réservée à un usage ultérieur

On peut représenter ces différentes classes par la figure suivante :

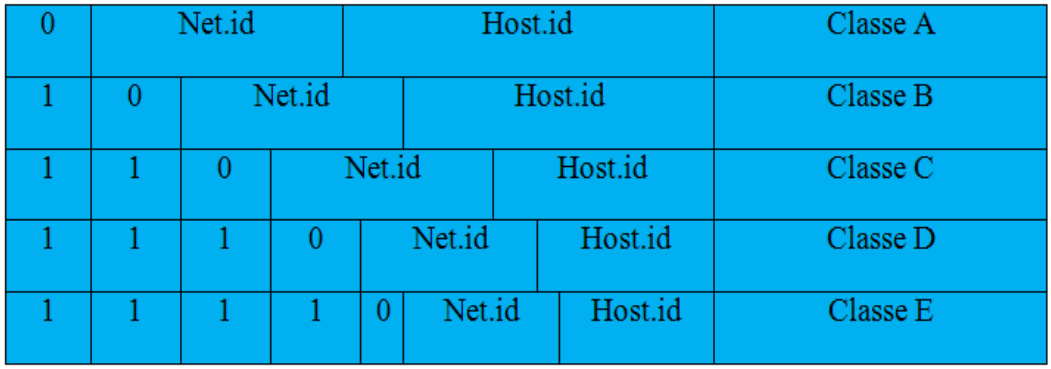

Figure 1.07 : *Classification d'adresse IP*

Pour définir la décomposition de l'adresse IP à 32 bits d'un ordinateur, un second numéro de 32 bits, appelé masque de sous-réseau, est utilisé. Ce masque fournit un guide pour l'interprétation de l'adresse IP. Il indique combien de bits sont réservés à l'identification du réseau dont fait partie l'ordinateur. La partie gauche du masque de sous-réseau est formée d'une série de 1 successifs. Tous les bits du masque qui correspondent à l'adresse du réseau ont la valeur 1, tandis que le reste du masque comporte des zéros. Les bits du masque de sous-réseau qui portent la valeur 0 identifient l'hôte. [4]

Pour la classe A, le masque de sous réseau est : 255.0.0.0

Pour la classe B, le masque de sous réseau est de 255.255.0.0

Pour la classe C, le masque de sous réseau est de 255.255.255.0

1.4.2.4.2 *Le routage*

Le routage consiste à trouver une ligne de sortie pour émettre et recevoir des données. Le but c'est de chercher le meilleur chemin possible pour acheminer les paquets. [8] [9]

On divise le routage en deux grandes familles :

- Le routage direct : Il s'agit de délivrer un datagramme `a une machine raccordée au même LAN.L'´emetteur trouve l'adresse physique du correspondant (ARP), encapsule le datagramme dans une trame et l'envoie.

- Le routage indirect : Le destinataire n'est pas sur le même LAN comme précédemment. Il est absolument nécessaire de franchir une passerelle connue d'avance ou d'employer un chemin par défaut.

Les opérations de routage se font grâce à une table, dite " table de routage ", dans une table de routage on peut trouver les champs suivants :

Destination : le réseau ou l'hôte de destination

Getway : la passerelle à employer pour atteindre la destination simplifiée

Flags : les flags décrivent certaines caractéristiques de cette route. Leurs valeurs possibles sont :

- D : La route a été crée dynamiquement
- G : La route désigne une passerelle, sinon c'est une route directe.
- H : La route est vers une machine, sinon elle est vers un réseau.
- L : Désigne la conversion vers une adresse physique
- S : La route a ´et´e ajoutée manuellement.
- U : La route est active.
- W : La route est le résultat d'un clonage.

Refcnt : Montre le nombre de fois qu'on a fait référence à la route pour établir une connexion

Use : Montre le nombre de paquets transmis via cette route

Interface : Le nom de l'interface réseau

Sous Unix, on tape la commande netstat-nr pour afficher une table de routage

Voici un exemple de table de routage

Henintsoa% netstat-nr

Routing tables

Destination	Getway	Flags	Rfcnt	Use	Interface
127.0.0.1	127.0.0.1	UH	1	298	lo0
192.168.192.10	8:0:9:85:76:9c	UHLW	2	50360	le0
Default	192.168.192.36	UGS	4	1179	le0
192.168.192.0	link#1	UC	10	1379	le0

- Numéros de protocole

Le numéro de protocole est un octet unique dans le troisième mot de l'en-tête du datagramme. La valeur identifie le protocole de la couche au-dessus d'IP à laquelle les données doivent être passées.

Sous Unix, les numéros de protocoles sont définis dans le fichier /etc/protocols. Ils s'agissent d'une simple table contenant le nom du protocole et le numéro associé. Le format de la table se compose d'un seul enregistrement par ligne, consistant du nom officiel du protocole et du numéro séparé par des espaces. Le numéro de protocole est séparé par des espaces de l' « alias » du nom du protocole. Les commentaires de table commencent par #

Un fichier /etc/protocols est représenté comme suit :

%cat /etc/protocols

Ip	0	IP
#hopopt	0	HOPOPT
Icmp	1	ICMP
Igmp	2	IGMP
Ggp	3	GGP
Ipencap	4	IP-ENCAP
St	5	ST
Tcp	6	TCP
Egp	8	EGP
Igp	9	IGP
Pup	12	PUP
Hmp	20	HMP
Xns-idp	22	xns-idp

- Numéro du port

Les numéros de port sont des valeurs de 16 bits qui identifient les processus d'application ou des services réseau. Dans chaque premier mot de l'en-tête de chaque datagramme TCP et chaque datagramme UDP existe le numéro de port source et numéros de port destination. Le numéro de port source identifie le processus ayant envoyé les données. Le numéro destination identifie les recevant.

Les numéros de port ne sont pas uniques entre les protocoles de transport.TCP et UDP peuvent se voir assigner les mêmes numéros de port. [10]

C'est la combinaison des numéros de port et de protocole qui identifie de manière unique le processus spécifique auquel les données doivent être délivrées. Sous Unix les numéros de port sont définis dans le fichier /etc/service. Voici un exemple :

henintsoa@debian :~$ cat /etc/services

Ldap	389/udp
Imsp	406/tcp
Imsp	406/udp
https	443/tcp
https	433/udp
snpp	444/tcp
snpp	444/udp
Microsoft-ds	445/tcp
Microsoft-ds	445/tcp
Kpasswd	464/tcp
Kpasswd	464/udp

Cette table combinée à celle de /etc/protocols, fournit toutes les informations nécessaires à l'acheminement des données vers l'application correcte

- Socket

La combinaison d'une adresse IP et d'un numéro de port est appelé socket.une socket identifie un processus réseau de façon unique dans tout l'Internet. Une paire de socket, l'une pour l'hôte récepteur et l'autre pour l'hôte émetteur, définit la connexion pour les protocoles orientés connexion comme TCP.

1.5 Architecture Client-serveur

1.5.1 *Présentation du système Client-serveur*

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en termes de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, … [7] [10]

Toutes les architectures informatiques Client/serveur présentes des caractéristiques communes :

Elles intègrent une interface utilisateur (UI) souvent graphique (GUI)

Elles fonctionnent grâce à des applications

Les applications qui les animent manipulent des données

C'est la répartition de ces 3 composantes entre le client ou le serveur qui caractérise les différentes architectures.

Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes. On parle ainsi, par exemple, de client FTP, client de messagerie, ..., lorsque l'on désigne un programme, tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès du serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client messagerie il s'agit de courrier électronique).

1.5.2 *Avantages et inconvénients du système Client-serveur*

Les avantages de ce système sont :

Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont:

Des ressources centralisées: étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction.

Une meilleure sécurité: car le nombre de points d'entrée permettant l'accès aux données est moins important. [7] [12]

Une administration au niveau serveur: les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés. [7] [12]

Un réseau évolutif: grâce à cette architecture on peut supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modifications majeures. [7] [12]

Les inconvénients sont :

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles:

Un coût élevé dû à la technicité du serveur

Un maillon faible: le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui. [7]

1.5.3 *Fonctionnement du système Client-serveur*

Un système client/serveur fonctionne selon le schéma suivant:

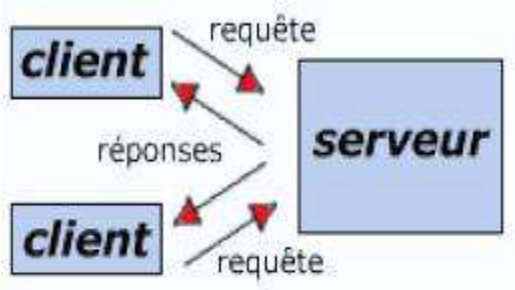

Figure 1.08 : *Fonctionnement du système client-serveur*

- Le client émet une requête vers le serveur grâce à son adresse et le port, qui désigne un service particulier du serveur
- Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine client et son port

1.5.3.1 Présentation de l'architecture à deux niveaux

L'architecture à deux niveaux (aussi appelée architecture 2-tier, tier signifiant étage en anglais) caractérise les systèmes clients/serveurs dans lesquels le client demande une ressource et le serveur la lui fournit directement. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir le service. [7] [11]

Voici une figure permet de représenter cette architecture à deux niveaux

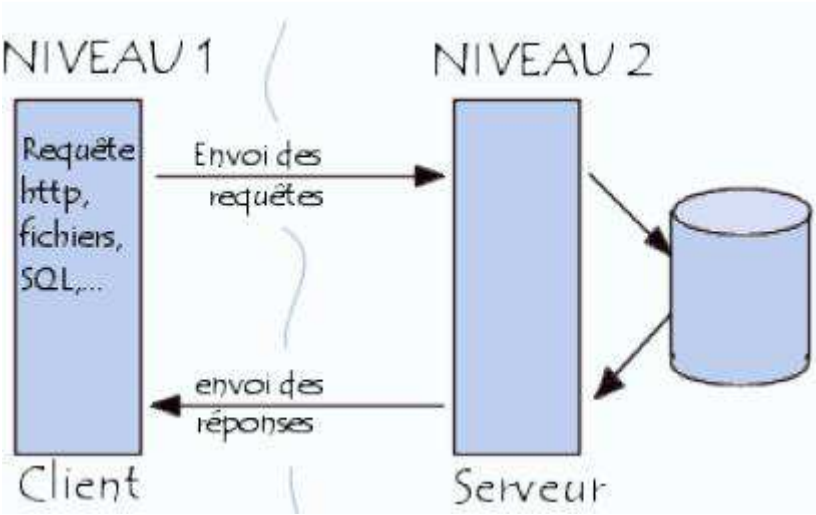

Figure 1.09 : *représentation de l'architecture à deux niveaux*

1.5.3.2 Présentation de l'architecture à trois niveaux

Dans l'architecture à 3 niveaux (appelées architecture 3-tiers), il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre:

Le client: le demandeur de ressources

Le serveur d'application (appelé aussi middleware): le serveur chargé de fournir la ressource mais faisant appel à un autre serveur

Le serveur secondaire (généralement un serveur de base de données), fournissant un service au premier serveur [11]

Voici une figure permettant de représenter cette architecture à trois niveaux

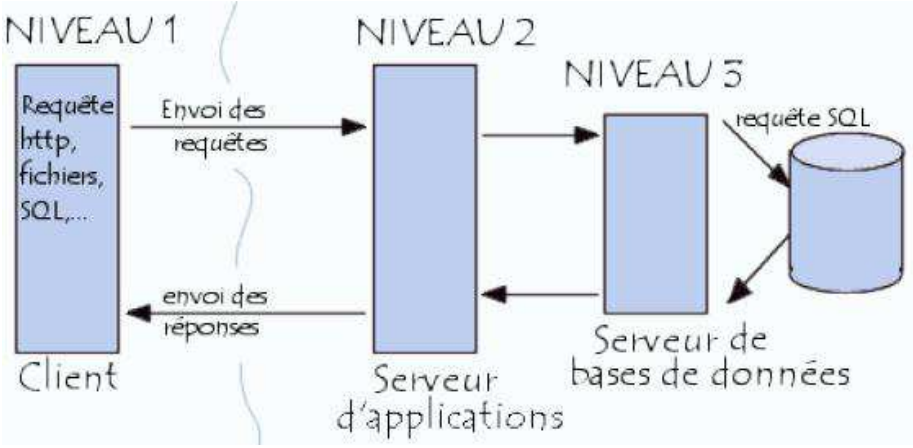

Figure 1.10 : *Représentation de l'architecture à trois niveaux*

Etant donné l'emploi massif du terme d'architecture à 3 niveaux, celui-ci peut parfois désigner aussi les architectures suivantes:

Partage d'application entre client, serveur intermédiaire, et serveur d'entreprise. [11]

Partage d'application entre client, base de données intermédiaire, et base de données d'entreprise.

L'architecture à deux niveaux est donc une architecture client/serveur dans laquelle le serveur est polyvalent, c'est-à-dire qu'il est capable de fournir directement l'ensemble des ressources demandées par le client. Dans l'architecture à trois niveaux par contre, les applications au niveau serveur sont délocalisées, c'est-à-dire que chaque serveur est spécialisé dans une tâche (serveur web/serveur de base de données par exemple). Ainsi, l'architecture à trois niveaux permet:

- Une plus grande flexibilité/souplesse [11]
- Une plus grande sécurité (la sécurité peut être définie pour chaque service) [11]
- De meilleures performances (les tâches sont partagées) [11]

1.5.3.3 Présentation de l'architecture à multi niveaux

Dans l'architecture à 3 niveaux, chaque serveur (niveaux 1 et 2) effectue une tâche (un service) spécialisée. Ainsi, un serveur peut utiliser les services d'un ou plusieurs autres serveurs afin de fournir son propre service. Par conséquence, l'architecture à trois niveaux est potentiellement une architecture à N niveaux...ou multi-niveaux. Voici une figure permet de représenter cette architecture à multi-niveaux

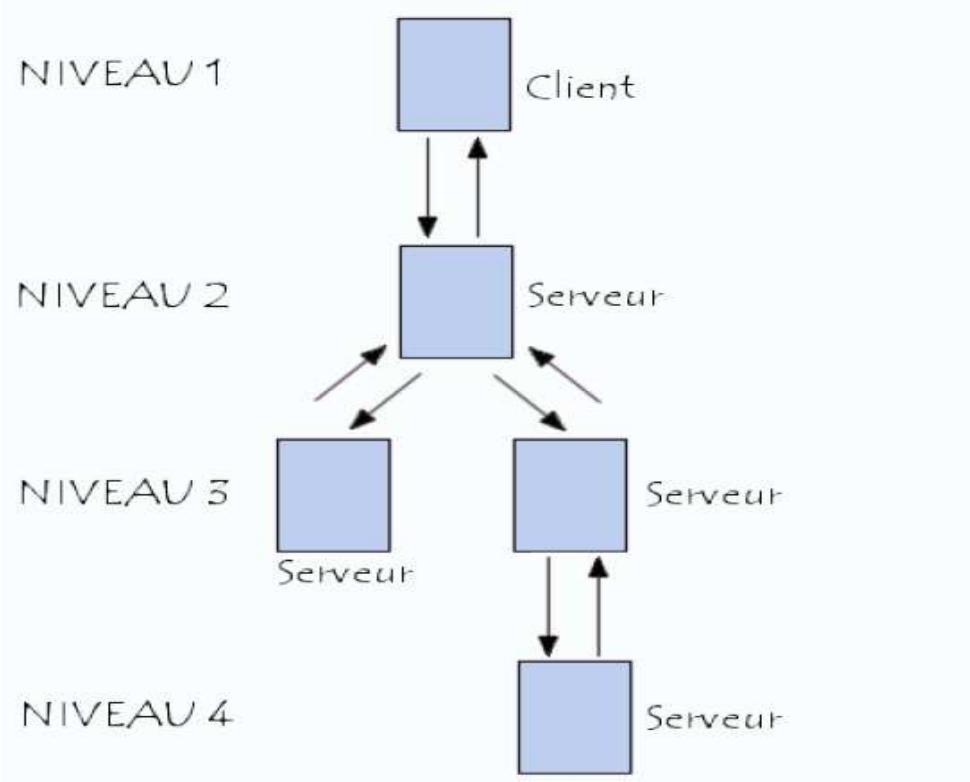

Figure 1.11 : *Architecture à multi-niveaux*

1.6 Conclusion

On peut en déduire que le réseau est une interconnexion des machines qui est nécessaire pour se communiquer, et pour assurer le bon transfert de l'information avec une quantité de service suffisante, il faut prévoir une architecture logicielle. Une normalisation de l'architecture logicielle s'impose, on distingue celui de l'ISO qui est l'OSI et celui du modèle TCP/IP. On a vue aussi que de nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes contactent un serveur, une machine généralement très puissante en termes de capacités d'entrée-sortie, qui leur fournit des services.

CHAPITRE 2

LE SYSTEME D'EXPLOITATION LINUX

2.1 Introduction

Linux est un système d'exploitation moderne bénéficiant de l'ensemble des fonctionnalités d'Unix. Ce n'est pas un produit commercial : c'est un logiciel libre que l'on peut obtenir gratuitement. Il est livré avec toutes les fonctionnalités, les outils et les utilitaires habituellement livrés avec les variantes commerciales d'Unix :

- C'est un système 32 bits ;
- Il est multiutilisateurs ;
- Il est multitâche ;
- Dans le domaine des réseaux, il prend parfaitement en charge la famille des protocoles TCP/IP et possède bien plus de caractéristiques que la plupart des variantes commerciales d'Unix ;
- Il dispose de shells très performants ainsi que de XFree86, une implémentation complète du système X−Window. [14] [15]

2.2 Pourquoi utiliser Linux comme serveur Intranet

2.2.1 Le système d'exploitation Linux

Linux est le système qui connaît actuellement le plus grand développement sur l'Internet ou Intranet. Principalement pour les raisons suivantes :

- Linux est le système de prédilection pour l'installation de trois logiciels serveurs leaders sur l'Internet : Apache en serveur Web, Postfix ou sendmail en serveur courrier et Bind en serveur DNS ;
- Le logiciel Samba qui lui permet d'être serveur de fichier et d'impression en environnement Microsoft ;
- La stabilité et la sécurité que lui confère le développement de son architecture et de ses modules au sein de la communauté Open Source.
- Le large choix d'applications dans de très nombreux domaines. Par exemple, la dernière distribution Debian donne accès à plus de 2000 logiciels différents.
- Moins d'interruptions de service grâce à une gestion intelligente de l'installation des logiciels. Un serveur sous Linux ne doit être redémarré que lors d'une modification matérielle comme l'ajout d'un disque ou d'une carte.

- Logiciel Libre. Linux est gratuit et librement récopiable. Cela signifie que l'on peut télécharger une version de Linux ou l'emprunter et l'installer sur n'importe quel nombre d'ordinateur.
- Accès aux sources des logiciels. Tous les utilisateurs peuvent modifier le fonctionnement des programmes ou engager un programmeur pour le faire. [14]
- Linux est plus efficace et consomme moins de ressources CPU et mémoire que Windows. On peut par exemple faire un serveur d'impression avec un vieux 486. [13] [14]

On peut résumer que Linux comme serveur permet d'avoir une réduction des couts, une sécurité et performance.

2.2.2 Linux et le serveur Apache

Le serveur Web Apache propose une qualité de service que peu d'offres commerciales peuvent concurrencer, [13] [14]

Apache tourne sur Unix, que ce soit Linux ou un UNIX BSD, ainsi que sur WindowsNT, W2K, et WXP. Une nette majorité des serveurs web tournent sous Unix, pour des raisons de performance et surtout de fiabilité. Le serveur Web Apache peut être utilisé comme simple serveur web, ou bien comme serveur d'application et interface de base de données avec les logiciels PHP et MySQL. De plus utiliser des logiciels libres, par opposition à des logiciels payants, est d'une part nettement moins cher, et un moyen de préserver l'indépendance technologique des pays. [14]

Linux en tant que serveur Intranet / Internet peut devenir l'ensemble des solutions suivantes et il est bien entendu possible qu'un seul et même ordinateur gère toutes ces possibilités :

- Un serveur WEB classique (HTTP) ;
- Un serveur FTP ;
- Un serveur de mail (SMTP, POP) ;
- Un serveur Proxy ;
- Un Firewall ;
- Un serveur DNS ;
- Un routeur, etc.…

Linux peut gérer un réseau d'entreprise, comme :

- Un serveur de fichiers ;
- Un serveur d'impression ;
- Un serveur de fax ;

- Un serveur de connexion Dial−Up (permet de devenir fournisseur d'accès à Internet)
- Un serveur de partage de connexion ;
- Un serveur de sauvegarde, etc. [13] [14]

Pour transformer, par exemple, un serveur Linux en serveur de base de données, il suffit de coupler le logiciel de base de données (comme MySQL) avec le serveur Web Apache via un langage comme PHP. Un simple navigateur Web suffit alors pour accéder à l'application voulue, ce qui permet d'alimenter et de consulter très facilement des bases de données.

2.3 Installation d'une distribution Linux

2.3.1 Première étape : vérifier son matériel

Pour installer Linux, une machine de type PC 386 ou plus dotée de 64Mo de mémoire vive est nécessaire. Il faut réserver un espace disque d'au moins 700 Mo (Sans environnement graphique, on peut se contenter de 32 Mo de mémoire vive et 300 Mo d'espace disque).

Avant d'installer Linux, il est recommandé de connaître les désignations de la carte graphique, de la carte Ethernet ainsi que de la carte son. Si on a déjà Windows installé sur la machine, il est mieux de rendre sur Panneau de Configuration, Système puis Gestionnaire de périphérique et de noter les références de la carte graphique, de la carte Ethernet ainsi que du carte son. Il est également à noter l'adresse IP si on bénéficie d'une adresse IP fixe, ce qui devrait être le cas si on souhaite installer un serveur Internet. [13] [14] [15]

2.3.2 Seconde étape : choisir sa distribution Linux

Quand on parle d'un système Linux, on fait un abus de langage. En effet Linux désigne seulement le kernel, une distribution englobe à la fois le kernel et les programmes permettant à l'utilisateur d'interagir avec le kernel. Chaque distribution a donc une certaine liberté dans la façon de présenter les commandes et sur le fonctionnement général du système. En particulier les programmes d'installation et de configuration sont souvent spécifiques à une distribution. [13]

Les distributions les plus connues sont :

- RedHat,
- Debian,
- Mandrake
- SuSE,
- Slackware,
- Corel Linux. [15]

2.3.3 Troisième étape : préparer ses disques durs

On peut installer Linux sur une partition DOS/Windows en utilisant par exemple Linux4win de Mandrake. Cette méthode est pratique car elle permet d'installer Linux sans partitionner son disque dur sur lequel est déjà installé Windows (Linux s'installe dans un unique fichier sur le disque Windows). Cette méthode présente le désavantage de ralentir le temps d'exécution de Linux.

Avant de commencer l'installation, on va devoir libérer de la place pour les nouvelles partitions Linux. Si on compte installer Linux sur un disque dur, pas de problème. Par contre, si on veut faire cohabiter Windows et Linux sur le même disque, et que Windows est déjà installé sur la totalité du disque, on va devoir passer de cette configuration :

A cette configuration :

Pour libérer de la place, il faut défragmenter au préalable le disque dur afin que toutes les données soient réunies au début du disque dur (sous Windows : Programme −> Accessoires −> Outil système −> défragmenteur de disque dur). Pour redimensionner le disque dur, on peut utilisez un logiciel approprié, comme Partition Magique. [13] [14]

Une autre possibilité pour repartitionner le disque dur est d'utiliser le programme FIPS qui se trouve dans le répertoire "tools" du premier CD de la distribution Debian.

2.3.4 Installation

Pour installer Linux, on doit démarrer la machine avec une version minimale de Linux. Pour cela trois méthodes sont possibles :

- Démarrer l'installation directement depuis le CD−ROM : le CD−ROM étant bootable, si votre Bios le permet vous pouvez booter directement sur le CD d'installation.
- Démarrer l'installation à partir de Windows : lors de l'insertion du CD−ROM d'installation depuis Windows, une fenêtre s'ouvre et on peut démarrer l'installation en cliquant sur le bouton "Complete Installation".
- Démarrer l'installation à partir d'une disquette de démarrage : sous Windows, lancer le programme rawritewin.exe du répertoire \dosutils du CD−ROM d'installation. Cliquez sur le bouton "…" à coté de "Image file" et sélectionnez le fichier cdrom.img du répertoire \images. Il ne reste plus qu'à cliquer sur le bouton "write" pour créer la disquette de boot. Redémarrer ensuite la machine avec la disquette crée.

Une fois l'installation lancée avec la méthode qu'on a choisi, un écran graphique Linux apparaît : appuyer sur la touche Entrée pour démarrer l'installation. Au bout de quelques secondes, la procédure d'installation démarre.

a) Choix de la langue : French / France

on doit ensuite valider la licence GPL, puis :

b) Classe d'installation : on a le choix entre une installation dite recommandée (installation standard), et une installation en mode expert. Si on a déjà une version antérieure de la Mandrake, on peut également effectuer une mise à jour du système ou uniquement des paquetages. Il est impérativement de choisir le mode expert afin de rester maître de l'installation (ce qui permet de choisir les paquetages à installer et de sélectionner manuellement le modèle de la carte graphique si sa détection automatique échoue).

c) Détection des disques durs : DrakX, le programme de configuration détecte automatiquement les périphériques PCI et SCSI du système. Si certains disques durs n'ont pas été détectés, on peut les sélectionner manuellement à partir d'une liste

d) Configuration de la souris : sélectionner le type du souris parmi la liste proposée. Si on ne sait pas quoi choisir, laisser la sélection proposée par défaut.

e) Choix du clavier : français puis cliquer sur "OK".

f) Sécurité : Laisser les options par défaut. Si on souhaite utiliser la machine en tant que serveur Internet, il est suggéré de choisir comme "niveau de sécurité" le mode "Plus élevé" afin d'obtenir un serveur vraiment sécurisé (dans ce mode, il n'est pas possible entre autre pour des raisons de sécurité de se connecter directement depuis l'extérieur sur la machine avec l'utilisateur root). Cependant si on débute, il est vivement conseillé de laiser le "niveau de sécurité" proposé par défaut et surtout pas le mode "paranoïaque" qui isole du réseau.

g) Système de fichiers : durant cette étape, on va créer les partitions nécessaires à Linux à partir de l'utilitaire DiskDrake. Attention à cette étape qui peut s'avérer dangereuse pour les données si on partage un même disque dur avec plusieurs systèmes d'exploitation (Windows et Linux par exemple). Il convient donc d'être très vigilant aux choix effectués.

Choisissez alors le disque dur où installer Linux (hda = premier disque dur IDE, hdb = second disque dur IDE, sda = premier disque dur SCSI, sdb = second disque dur SCSI, etc..).

Si on n'a pas de disque dur ou de partition disponible pour installer Linux, il nous faut alors redimensionner la partition existante : attention avant de redimensionner la partition Windows, il est nécessaire de fragmenter le disque dur afin que tous les fichiers soient situés au début du disque dur et non en vrac sur l'ensemble du disque dur. Il est également fortement conseillé de sauvegarder ses données au préalable.

Une fois identifié ou créé une partition dédiée à Linux, il faut segmenter l'espace disponible pour Linux en trois partitions :

une partition de type Ext2 (linux native) pour la racine du système avec / comme point de montage (cette partition sert aux fichiers systèmes), une partition de type Swap (linux swap) pour

la mémoire virtuelle du système (il est recommandé d'allouer une taille équivalente au double de la mémoire vive disponible), et enfin une partition de type Ext2 (linux native) pour les répertoires utilisateurs avec /home comme point de montage.

A noter qu'on peut également utiliser le mode "Partitionnement automatique" si on préfère laisser au système le choix du paramétrage des partitions. Si on a un quelconque doute durant cette étape et si on utilise un même disque dur pour Windows et Linux, il est conseillé de rebooter la machine et d'effectuer une sauvegarde préalable de toutes les données.

Une fois terminé la configuration des partitions nécessaires à Linux, cliquer sur le bouton "Terminer" pour la création effective des partitions. En fonction des choix effectués, il est possible que le système demande alors de redémarrer la machine pour prendre en considération les partitions nouvellement créées (on doit alors relancer la procédure d'installation à partir du CD−ROM de démarrage, de la disquette de démarrage ou depuis Windows : l'installation redémarre

Formatage des partitions : le programme d'installation propose par défaut de formater la partition racine, la partition utilisateurs et la partition de swap nécessaires à Linux. Cliquez sur "OK" pour lancer le formatage de ces partitions. Si on a Windows installé, ne cliquer surtout pas sur la partition /mnt/windows ce qui aurait pour effet de supprimer toutes les données de Windows La vérification de la présence de blocs endommagés n'est pas indispensable : sélectionner des partitions à vérifier si on a des doutes sur l'intégrité du disque dur (on peut tout de même vérifier les partitions racine et utilisateurs)

h) Choix des paquetages : durant cette étape, on peut sélectionner les applications qu'on souhaite installer ou non sur le système. On risque d'être fort impressionné voire désappointé par le grand nombre d'applications disponibles aussi si on n'a pas besoin d'applications particulières telles que des logiciels de gravure de CD, on peut se contenter des choix par défaut.

Pour les besoins serveur, on recommande de sélectionner les paquetages de la rubrique "Serveur".

A noter que si on utilise à la fois Windows et Linux sur la même machine, on peut également ajouter Wine de la rubrique Emulators si on souhaite exécuter des applications Windows depuis Linux.

A l'issu de la validation des choix, le système copie sur le disque durs tous les paquetages sélectionnées. Cette étape dure une dizaine de minute en fonction du nombre de paquetages sélectionnés.

i) Mot de passe du root : pour d'évidentes raisons de sécurité le mot de passe du root doit être compliqué et il faut à tout pris éviter de se contenter d'un prénom, d'une date de naissance et même de l'assemblage de mots existants dans un dictionnaire (des logiciels sont spécialisés dans la recherche automatique de mots de passe par simple assemblage de mots du dictionnaire). Il est donc conseillé d'utiliser à la fois des caractères en minuscules et en majuscule, des chiffres et des symboles. Un mot de passe tel que KaOuaga32 ! ne pourra pas être déterminé par des programmes de recherche de mot de passe.

j) Ajout des utilisateurs : vous pouvez ajouter des utilisateurs lors de cette étape ou par la suite à tout moment.

On suggère d'ajouter au moins un utilisateur ne serait−ce que parce que si on a opté pour le niveau de sécurité dit "paranoïaque", il ne sera pas possible d'effectuer un accès distant sur la machine à partir du compte root .Cliquer ensuite sur "Terminer" pour passer à l'étape suivante.

k) Configuration du réseau : avec la version 9.0, cette étape est extrêmement simplifié puisqu'il suffit de suivre l'assistant automatique et de vérifier que le choix proposé correspond bien à votre configuration !

Configuration du périphérique réseau eth0 : on doit spécifier l'adresse IP de votre réseau. Etant donnée qu'on souhaite installer un serveur Internet (ou Intranet), on devra logiquement avoir une adresse IP fixe ou en utilisant le service DHCP.

On doit ensuite spécifier le nom du machine sous forme:

nom−de−la−machine.nom−du−domaine.top−level−domain (par exemple henintsoa.africacomputing.org pour spécifier que la machine s'appelle henintsoa et fait partie du domaine africacomputing.org), ainsi qu'éventuellement l'adresse IP de la passerelle si on utilise par exemple un routeur pour accéder à l'extérieur, puis du proxy si on en a un.

l) Configuration des services : cette étape permet de sélectionner les services qui seront lancés automatiquement lors du démarrage du système. Les choix proposés conviennent pour la plupart des besoins. Si on souhaite utiliser un serveur LDAP, on peut rajouter ce service dès à présent. De même si on souhaite utiliser un serveur DNS, on peut ajouter le service "named" dès à présent.

m) Programme d'amorçage : si on utilise plusieurs systèmes d'exploitation sur la même machine, on a la possibilité d'installer un chargeur de démarrage qui permettra de choisir au démarrage quel système d'exploitation on souhaite lancer. Si on a plusieurs systèmes d'exploitation on fera mieux d'installer Grub, sinon cliquez simplement sur "Aucun".

Si on utilise Lilo et qu'on installe Linux sur le même disque que Windows, spécifiez le partition root Linux comme support de boot car le Master Boot Record du disque dur est déjà occupé par celui de Windows.

n) Disquette de démarrage : comme pour l'installation de tout OS, il est fortement recommandé d'effectuer une disquette de démarrage au cas où on aurait un problème pour démarrer directement à partir du disque dur.

o) Configuration X : il s'agit de la configuration de la carte graphique. Nécessaire pour l'exécution de Xfree86, l'implémentation Linux de l'environnement graphique X−Window. Sélectionnez le pilote de la carte graphique en appuyant sur la désignation de la carte. Puis sélectionnez un pilote pour le moniteur, puis la résolution graphique et enfin testez si la configuration fonctionne. Activez enfin le lancement de l'interface graphique au démarrage si on souhaite utiliser la machine en local (c'est à dire autrement qu'à partir d'une connexion distante).

2.4 Utilisation de Linux

2.4.1 Introduction

Linux est un système d'exploitation puissant mais son utilisation n'est pas facile surtout pour les utilisateurs non familiarisés avec l'environnement UNIX. L'utilisation de la plupart des applications peut s'effectuer à partir de l'interface graphique X−Window (ou à partir de sur−couches de X−Window telles que les environnements graphiques KDE et GNOME). Cependant pour certains travaux, il est beaucoup plus pratique et plus souple d'utiliser des lignes de commande depuis un environnement shell plutôt que d'utiliser de lourdes solutions graphiques. De plus, si on doit intervenir sur un serveur Linux à distance (c'est à dire depuis un poste connecté à Internet), on doit inévitablement devoir utiliser des lignes de commande.

Un shell est la liaison la plus élémentaire entre l'utilisateur et le système d'exploitation, c'est à dire le programme de gestion de la ligne de commande. Les commandes saisies sont interprétées par le shell et transmises au système d'exploitation. [14]

De nombreuses commandes du shell ressemblent aux commandes MS−DOS : en utilisant la terminologie UNIX,on peut considérer que le programme command.com correspond au shell de MS−DOS. Dans les environnements de type UNIX, il existe plusieurs shells (bash, tcsh, csh, sh, etc.). [14] [15]

2.4.2 Système de fichier

L'entrée du système se situe à la racine, notée / et il existe un certain nombre de répertoire par défaut comme : /boot, /bin, /dev, /etc, /home, /lib, /lost + found, /media, /mnt, /proc, /root, /sbin, /sys, /tmp, /usr, /var. [16]

2.4.3 Les commandes de base

Pour toutes les commandes, il est possible d'obtenir de l'aide en tapant man suivi du nom de la commande. En tapant une commande suivie du paramètre − −help, on obtient la liste des paramètres possibles. Lorsqu'on a besoin d'aide sur l'utilisation ou la syntaxe des commandes, il ne faut pas hésiter à recourir à la commande man ou au paramètre − −help dès qu'on a besoin d'aide.

Voici quelques commandes les plus utilisées en Linux :

- Cat , more : permettent d'afficher les contenus d'un fichier. La commande cat permet de visualiser le contenu d'un fichier c'est à dire d'envoyer le contenu du fichier vers une la sortie par défaut : l'écran. La commande more permet également de visualiser le contenu d'un fichier. L'affichage s'effectue page par page. [16]
- Vi et emacs : permettent d'éditer un fichier.vi est l'éditeur élémentaire que l'on retrouve sur la plupart des systèmes d'exploitation et qui n'utilise pas d'interface graphique. Il prend en charge les commandes et les données en même temps. Une fois vi lancé, deux modes de fonctionnement se présentent : le mode commandes et le mode édition. [16]

  · Pour passer du mode édition au mode commande il suffit d'appuyer sur la touche échappement ;

  · Pour passer du mode commande au mode édition il faut taper la commande d'insertion (ou équivalent)

  emacs est un autre éditeur standard utilisé dans différents systèmes d'exploitation, il dispose d'un langage qui permet de le personnaliser à souhaits. Il dispose néanmoins de menus 'habituels' tels que la gestion des fichiers, la recherche de caractères, etc. Ainsi que de règles préprogrammées qui permettent aux développeurs une mise en page dépendante du langage utilisé (C, C++, java ...) reconnaissant les commandes courantes, les chaînes de caractères, etc...
- find et which : permettent de trouver un fichier. Il arrive que l'on ait à retrouver un fichier dont on ne connaît plus l'emplacement ou même le nom ; Linux comprend quelques outils pour ces recherches. [16]

  La commande which permet de scruter les répertoires les plus communément utilisés (dont le chemin est indiqué dans la variable d'environnement PATH) pour retrouver le nom de fichier indiqué en argument. Cette commande est surtout utile pour vérifier que l'on utilise bien la version souhaitée d'un binaire (exécutable). La commande whereis est semblable à la commande which. [15]
- Grep : permet de trouver un texte dans un fichier

- Ln : pour le lien. La création de liens symboliques (opposition aux liens physiques) évite la copie de fichiers identiques dans différents répertoires. Par exemple, si une application a besoin d'un fichier volumineux contenant des données relatives à un groupe d'utilisateurs, il est possible de l'avoir virtuellement dans les répertoires courant en créant un lien symbolique. [15] [16]
- Df et du : permettent de connaitre l'espace disque restant. La commande df renseigne sur l'espace disque total, disponible (disk free). Elle s'utilise sur tous répertoires "montés". Cette commande s'utilise généralement avec en argument le nom d'un fichier pour vérifier le point de montage de son répertoire.
- Cd : permet de se déplacer dans un répertoire. La commande cd permet de se déplacer dans les répertoires. La commande ls permet d'afficher la liste des fichiers d'un répertoire.
- Chmod : permet de modifier le droit d'accès
- Cp, rm, mv : permettent de copier, supprimer, déplacer et renommer un répertoire. [13] [15]

2.4.4 Archiver, compresser et décompresser

Archivage de fichiers :

Pour archiver des fichiers, on assemble le groupe de fichiers à archiver :

tar <destination> <sources>

Assemblage des différents fichiers (fichier i) dans monfichier :

$ tar −cf monfichier.tar fichier1 fichier2 ... fichiern

Pour assembler en récursif (avec les sous−répertoire) des répertoires :

$ tar −cf monfichier.tar rep1 rep2 ... repn

Désassemblage :

$ tar −xf <monfichier.tar>

Compression d'un fichier :

Une commande de compression permettra ensuite de diminuer la taille totale de ces fichiers assemblés : gzip, compresse monfichier et le remplace par le fichier monfichier.gz : gzip monfichier

Pour décompresser un fichier archive essayer la commande suivante : gzip −d fichier.gz

Ainsi l'on peut assembler et compresser les fichiers à archiver. La commande tar xvfz permet de décompresser en même temps que le désassemblage. [13]

On peut écrire aussi un script sur linux. Un script est une suite d'instruction élémentaire qui est exécutées de façon séquentielle (les unes après les autres) par le langage de script. [10]. Pour cela on tape la commande vim et on met une extension, parfois l'extension la plus utilisée est le sh.

2.4.5 Installation d'un logiciel et Linux en réseau

2.4.5.1 Installation d'un logiciel

L'installation de nouveaux logiciels s'effectue soit à partir des sources, soit à partir d'un binaire (application déjà compilée), soit à partir d'un paquetage rpm.

a) Installation à partir des sources

L'installation à partir des sources consiste à compiler des lignes de code (en C ou en C++) puis à installer le binaire produit. Les avantages de cette méthode sont multiples :

- un même code source peut être compilé sur n'importe quelle machine UNIX et ce quel que soit son processeur (Intel, Alpha, Risc, PowerPC, etc..) ;
- vous pouvez spécifier le répertoire où l'application doit être installée ;
- vous pouvez compiler l'application avec des options spécifiques (ajout de modules particuliers, optimisation du binaire en fonction du processeur, etc...)
- les sources étant moins volumineux que les binaires, le téléchargement des sources d'une application est beaucoup plus rapide que le téléchargement du binaire ou du paquetage rpm correspondant.

Qu'elle que soit l'application, la procédure d'installation est identique :

- Préparation de la compilation par la commande : $ ./configure -prefix=répertoire-de-destination
- Compilation de l'application par la commande : $ make
- Installation de l'application par la commande : $ make install

Il ne reste ensuite plus qu'à exécuter le script de lancement de l'application et si la nouvelle application doit être lancée systématiquement au démarrage de la machine (cas des services Internet), il faut également copier le script de lancement dans le répertoire /etc/rc.d/init.d.

b) Installation à partir d'un binaire

Pour une application donnée, il existe peut être déjà une version binaire compilée pour le processeur. Il ne reste plus qu'à télécharger l'application, la décompresser puis la déplacer dans le répertoire choisi. A noter que dans la désignation employée dans les distributions binaires : Intel-386 désigne un processeur Intel de type 386, intel-486 de type 486, intel-586 de type Pentium, intel-686 de type Pentium II, etc...
Tout comme pour une installation à partir des sources, on doit ensuite lancer l'application et vérifier le cas échéant si celle-ci est lancée au démarrage.

c) Installation à partir d'un paquetage rpm

RPM est un puissant gestionnaire d'applications permettant d'installer, de mettre à jour, de vérifier ou de désinstaller des composants logiciels.

Pour installer un nouveau paquetage appli.rpm :

$ rpm -ivh appli.rpm

Attention, si on installe un paquetage par cette méthode et qu'il existe déjà sur le système dans une version inférieure, on risque d'avoir des problèmes pour le désinstaller. Les paramètres -vh permettent d'ajouter une barre de progression.

Pour mettre à jour (upgrader) un paquetage :

$ rpm -Uvh appli.rpm

Pour supprimer un paquetage :

$ rpm -e appli.rpm

Afficher la liste de tous les paquetages installés :

$ rpm -qa

Vérifier à partir du nom si un paquetage est déjà installé :

$ rpm -qa | grep php

Lister le contenu d'un paquetage :

$ rpm -ql appli.rpm

2.4.5.2 Linux en réseau

a) *Outils réseaux*

Linux contient de nombreux utilitaires permettant de faciliter l'administration d'un réseau.

ifconfig : utilitaire standard UNIX permettant d'obtenir des informations sur la configuration de l'interface réseau (carte Ethernet par exemple) : `$ ifconfig -a`
netstat : utilitaire de surveillance d'un réseau sous les systèmes UNIX.

ping : l'outil le plus simple et le plus pratique des outils réseaux. ping permet de vérifier si un nom d'hôte distant ou une adresse IP est accessible.

traceroute : utilitaire très utile pour diagnostiquer des problèmes réseaux, en particulier si la commande ping ne réussit pas à atteindre le serveur distant. Il existe des traceroute graphiques permettant de visualiser le chemin parcouru par les données entre un client et un serveur.

b) *Configuration d'un réseau local sous Linux*

Interface réseau : l'interface réseau est représentée physiquement par votre carte réseau mais le terme interface réseau est aussi utilisé pour désigner un nom logiciel auquel assigner une adresse IP (eth0 par exemple). Une adresse IP est toujours assignée à une interface réseau, jamais à un ordinateur. La commande ifconfig sert à afficher la configuration des différentes interfaces réseau actives.

Fichiers de configuration :

/etc/hosts : ce fichier spécifie comment résoudre les noms des machines du réseau local (inutile de mettre en œuvre un serveur DNS pour un petit réseau local). La syntaxe des lignes de ce fichier est :

Adresse IP	Nom de l'hôte	Alias
127.0.0.1	localhost	
192.168.0.1	sirius.mondomainesirius	

/etc/resolv.conf : ce fichier spécifie où résoudre ce qui ne se trouve pas dans `/etc/hosts`. C'est dans ce fichier que vous devez spécifier les adresses IP des serveurs DNS utilisés pour accéder à Internet en suivant la syntaxe suivante : nameserver 212.102.31.1

/etc/HOSTNAME (ou /etc/sysconfig/network sur certaines distributions) : ce fichier configure le nom de la machine locale. Au démarrage du système, ce fichier est lu et son contenu est envoyé à la commande hostname. [13] [14]

2.5 Conclusion

Linux est un système d'exploitation le plus utilisé actuellement, son utilisation peut se faire par une interface graphique ou par des lignes de commande. Ce chapitre nous permet de connaitre le système d'exploitation linux, son utilisation et ses avantages par rapport à d'autres systèmes d'exploitation.

CHAPITRE 3

SECURISATION DES RESEAUX

3.1 Introduction

Le réseau local d'une entreprise est souvent connecté à internet pour avoir les différents nouveaux services que l'internet offre, ce qui implique un bon nombre d'utilisateur qui peut venir chez soi. Pour cela il est nécessaire de sécuriser le réseau local de cette entreprise. Ce chapitre nous permet de voir quels sont les types d'attaques, qui sont les agresseurs et comment fait-on pour en protéger.

3.2 Qu'essayons-nous de protéger

Quand nous nous connectons à l'Internet, nous risquons de perdre :

Nos ressources : Nos ressources informatiques c'est-à-dire notre machine, nos réseaux et même notre énergie

- Notre réputation : Si un intrus apparait à l'internet avec votre identité, tout ce qu'il fait semble provenir de vous et les conséquences sont majeures : d'abord dans la plupart du temps, d'autres sites ou des organismes de sécurité nationale commencent à vous appeler pour vous demander pourquoi vous essayez de pénétrer dans leurs systèmes. [17] [19]
- Si un intrus qui vous déteste activement peut envoyer des messages électroniques, poster des articles de news qui paraissent venir de vous. Les gens qui choisissent ceci recherchent l'animosité maximale plus que la crédibilité, mais même si quelques personnes croient ces messages, le nettoyage peut être long et humiliant. [18] [19]
- Nos données : nos données possèdent trois caractéristiques distinctes qui justifient leur protection :
    - Le secret : nous ne désirons probablement pas que d'autres personnes les connaissent
    - L'intégrité : nous ne désirons probablement pas que quelqu'un d'autres les modifie
    - La disponibilité : nous désirons presque certainement les utiliser nous mêmes

Pour sécuriser un réseau, il faut bien connaitre les types d'attaques ou d'agresseur qui endommagent le système ou le réseau [17] [19]

3.3 Contre qui essayons – nous de protéger

Quels types d'attaques devrions – nous affronter sur l'Internet, et quels types d'attaquants sont susceptibles de les lancer.

3.3.1 Types d'attaques

Il existe de nombreux types d'attaques système, et nombreuses manières de les classer. Nous séparons les attaques en trois grandes catégories : intrusion, vol d'informations et refus de service

Intrusion : l'intrusion est les attaques les plus courant dans nos système ; avec les intrusions, les gens sont réellement capables d'utiliser vos ordinateurs. La plupart des intrus veulent utiliser vos ordinateurs comme s'ils étaient les utilisateurs légitimes donc ils ont un accès direct sur vos données. [19]

Vol d'informations : certains types d'attaques permettant à un agresseur d'obtenir des données sans en passer par l'utilisation directe de vos ordinateurs. Ces attaques exploitent en général des services Internet qui sont censés donner des informations, les conduisant à en fournir plus que ce qui est prévue, ou à les fournir à des gens non autorisés. De nombreux services Internet sont conçus pour être utilisés sur des réseaux locaux, et ne possède pas le type ou le degré de sécurité qui leur permettrait d'être utilisé da façon sûre sur l'Internet [19]

Refus de service : Une attaque par refus de service a pour seul et unique but de vous empêcher de vous servir de vos propres ordinateurs. Globalement, une attaque de refus service provoque un dérangement où interrompt totalement la fourniture des services à des utilisateurs, des réseaux, de systèmes ou d'autres ressources légitimes. [19]

Les types d'attaques de refus de service sont :

- La consommation de bande passante : pour cela les attaquants parviennent à inonder la connexion réseau de la victime parce qu'ils disposent de plus de bande passante que celle-ci. Par exemple, quelqu'un qui possède une connexion réseau par exemple de 1544 Mbps ou plus inonde une liaison qui possède 128 Kbps.
- Epuisement des ressources : cette attaque se distingue d'une attaque par consommation de bande passante dans la mesure où elle se concentre sur la consommation de ressource système et non du réseau. Généralement, elle indique la consommation de ressource système, notamment l'utilisation de CPU, RAM,…
- Défaut de programmation : les défauts de programmation sont des incapacités à gérer des conditions exceptionnelles liés à une application, à un système d'exploitation. Ces conditions exceptionnelles résultent généralement de l'envoi par un utilisateur de données non prévues vers l'élément vulnérable.

- Attaque par routage et DNS : une attaque par routage implique la présence des pirates manipulant les entrées de la table de routage pour refuser la fourniture de services à des systèmes ou réseaux. Les attaques de refus de services DNS nécessitent de convaincre le serveur victime d'enregistrer des informations fictives. Lorsqu'un serveur DNS effectue des vérifications, les pirates peuvent réacheminer les données vers le site de leur choix ou, dans certains cas vers un trou noir. [17] [19]

Voici quelques exemples des attaques, le plus souvent, par internet:

- Les attaques par ICMPr :

Le protocole ICMP est utilisé par les routeurs pour transmettre des messages de supervision permettant, par exemple, d'indiquer à un utilisateur la raison d'un problème. Un premier type d'attaque contre un serveur consiste à générer des messages ICMP en grande quantité et de les envoyer au serveur à partir d'un nombre des sites importants. . Pour inonder un serveur, le moyen le plus simple est de lui envoyer des messages de type ping demandant au serveur de renvoyer une réponse. On peut également inonder un serveur par des messages de contrôle ICMP d'autres types. [9]

- Les attaques par TCP :

Le protocole TCP travaille avec des numéros de port qui permettent de déterminer une adresse de socket, c'est-à-dire d'un point d'accès au réseau. Cette adresse de socket est formée par la concaténation de l'adresse IP et de l'adresse de port. A chaque application correspond un numéro de port, par exemple 80 est destiné pour une application http. [9]

Une attaque par TCP revient à utiliser un point d'accès pour faire autre chose que ce quoi le point d'accès a été défini. En particulier, un pirate peut utiliser un port classique pour entrer dans un ordinateur ou dans une entreprise. La figure suivante illustre ce type d'attaque.

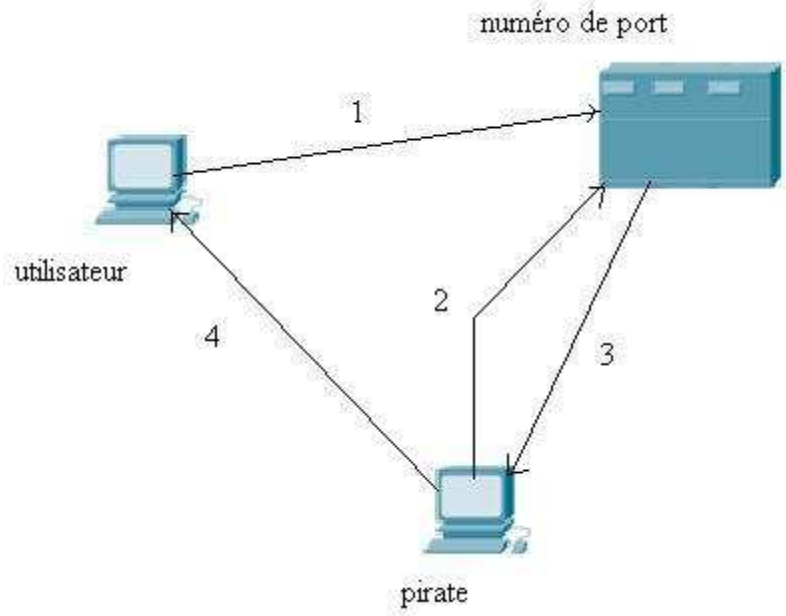

Figure 2.01 : *une attaque par le protocole TCP*

1 : ouverture d'une connexion TCP

2 : Prise de la communication par le pirate

3 : Communication entre le serveur et le pirate

4 : Eventuellement retransmission vers l'utilisateur

Dans cette figure, l'utilisateur ouvre une connexion TCP sur un port correspondant à l'application qu'il projette de dérouter. Le pirate commence à utiliser le même port en se faisant passer pour l'utilisateur et se fait envoyer les réponses. Eventuellement, le pirate peut prolonger les réponses vers l'utilisateur de telle sorte que celui-ci reçoive bien l'information demandée et ne puisse pas se douter de quelque chose.

- Les attaques par cheval de Troie

Le nom de cette attaque provient de la ruse imaginée par l'Ulysse durant la guerre de Troie par laquelle la ville avait été prise en faisant entrer dans ces murs un grand cheval en bois rempli des soldats. [9]

Dans l'attaque par cheval de Troie, le pirate introduit dans la station terminale un programme qui permet de mémoriser le login et le mot de passe. Ces informations sont envoyées vers l'extérieur par un message sur une boite aux lettres anonymes. Diverses techniques peuvent être utilisées pour cela, allant d'un programme qui remplace les gestionnaires de login jusqu'à un programme pirate qui espionne ce qui se passe dans le terminal

- Les attaques par dictionnaire :

Beaucoup de mot de passe sont choisis dans le dictionnaire, et il est donc très simple pour un automate de les essayer tous. De nombreuses expériences ont démontré la facilité de cette

attaque et ont mesuré que la découverte de la moitié des mots de passe des employés d'une grande entreprise s'effectuait en moins de deux heures.

Une solution simple pour remédier à cette attaque est bien sûr de complexifier les mots de passe en leur ajoutant des lettres majuscules, des chiffres et des signes comme !, ?, &, etc. [9]

- Les autres attaques :

Le nombre d'attaques possibles est bien trop grand pour que nous puissions les citer toutes. De plus, de nouvelles procédures d'attaques s'inventent chaque jour, néanmoins on va citer quelques uns [9]

Les attaques par écoute consistent, pour un pirate, à écouter une ligne de communication et à interpréter les éléments binaires qu'il intercepte. Les attaques par fragmentation utilisent le fait que les informations de reconnaissance se trouvent dans le premier paquet provenant de la fragmentation d'un message. Un pirate peut modifier la valeur bit de fragmentation, ce qui a pour effet croire que le message n'est pas fait d'un seul segment mais de plusieurs.

Les algorithmes de routage sont à la base de nombreuses attaques. En effet, en effectuant des modifications sur les tables de routage. Le pirate peut récupérer de nombreuses informations qui ne lui sont pas destinées.

De la même façon, de nombreuses attaques sont possibles en perturbant un protocole comme ARP, soit pour prendre place d'un utilisateur, soit en captant des données destinées à un autre. [9]

3.3.2 Types d'agresseurs

Les types d'agresseur qu'on décrit ici sont ceux que l'on trouve sur l'Internet. Tous partagent un certain nombre de caractéristiques. Ils ne veulent pas être pris, ce qui les pousse à se cacher. S'ils obtiennent l'accès à un système, ils essayeront certainement de préserver cet accès et si possibles en réalisant d'autres moyens d'accès. La plupart d'entre eux sont en contact avec d'autres personnes qui partagent le même genre d'intérêt, et la plupart partageront les informations qu'ils obtiendront d'un système. Connaissant ces types d'attaques et ces types d'agresseurs, que ce qu'on doit faire pour en protéger ?

3.4 Comment protéger les sites

Pour protéger contre ces genres d'attaques, on peut choisir entre de nombreux modèles de sécurité : de l'absence pure et simple à la sécurité réseau, en passant, par ce que l'on appelle sécurité par l'obscurité et la sécurisation des serveurs.

3.4.1 Absence de sécurité

L'approche la plus simple consiste à ne faire aucun effort en matière de sécurité, et de ne faire tourner que ce que le vendeur fournit par défaut. [19]

3.4.2 Sécurité par l'obscurité

La sécurité par l'obscurité est un autre modèle de sécurité. Elle suppose qu'un système est sûr si personne ne le connait, qu'il s'agisse de son existence, de son contenu ou de quoi que soit d'autre. Mais la possibilité est critique car il existe beaucoup trop de manières de trouver une cible attrayante. Par exemple, pour fonctionner sur un réseau, internet inclus, un site doit se soumettre à une procédure minimale d'enregistrement, et une grande partie de ces informations sont disponibles à quiconque en fait la demande. Chaque fois qu'un site utilise des services sur le réseau, quelqu'un ou tout au moins celui qui fournit le service sait que ce site est présent. Les intrus regardent les nouvelles connexions, dans l'espoir que ces sites n'auront pas encore mis en place de nouvelles mesures de sécurité. Certains ont rapporté la présence de sondes apparemment basés sur les apparitions de nouveaux sites. La connaissance du matériel installé et du logiciel, et de la version du système d'exploitation sous lequel vous tournez, donne aux intrus de précieux indices sur les trous de sécurité qu'ils peuvent tenter d'exploiter. Ils peuvent souvent obtenir ces informations d'après vos données d'enregistrement, ou en essayant de se connecter à un ordinateur

De nombreux systèmes affichent ce type d'information avec le message de login, ce qui fait qu'un intrus n'a même pas besoin d'y accéder.

Les agresseurs ont le temps de leur coté, et peuvent souvent éviter de se perdre dans des méandres de conjoncture en se contentant d'essayer toutes les possibilités. Au bout du compte, l'obscurité n'est pas un choix stratégique valable. [19]

3.4.3 Sécurité par l'hôte

Le modèle le plus courant de sécurité informatique consiste à sécuriser les serveurs. Dans ce modèle, on renforce séparément la sécurité de chaque machine hôte. Mais le problème est la complexité et la diversité des serveurs. La plupart d'entre eux comprennent des machines de diverses provenances, chacune avec son propre configuration et son propre système. Même si le site est constitué de machines provenant d'un seul constructeur ou fournisseur, les différentes versions d'un même système d'exploitation ont souvent des problèmes de sécurité distincts. Et même si les machines tournent toutes avec un même système d'exploitation, les différentes configurations peuvent faire rentrer différents sous-systèmes en jeu et mener à d'autres types de problèmes. Tout ça implique que la sécurisation d'une machine est bien plus difficile que son

rattachement à un réseau. Un modèle de sécurité par serveur peut être tout à fait approprié pour des petits sites, ou pour ceux qui nécessitent une sécurisation extrême. En fait, tous les sites, doivent comprendre un certain niveau de sécurité par hôte dans leur planification générale. [19]

3.4.4 Sécurité par réseau

Au fur et à mesure que les environnements croissent en taille et en diversité, et que leur sécurisation machine par machine devient plus difficile. De plus en plus, les sites se tournent vers un modèle de sécurité par réseau. Dans ce dernier, on se concentre sur le contrôle de l'accès réseau aux divers serveurs et aux services qu'ils offrent au lieu de les sécuriser un par un. Les approches de sécurité réseau comprennent la réalisation de firewalls qui protègent les systèmes et les réseaux internes en utilisant des principes d'authentification puissants, ainsi que le chiffrement des données sensibles pendant qu'elles traversent un réseau. [19]

Un site peut être remarquablement soulagé de ses efforts de sécurisation en utilisant un modèle de sécurité par réseau. Le firewall est une des méthodes de la sécurité par réseau.

Il faut noter qu'aucun modèle de sécurité ne peut résoudre tous les problèmes, aucun modèle de sécurité ne peut empêcher une personne hostile disposant d'un accès légitime d'endommager volontairement le site ou d'en sortir des informations confidentielles mais on peut espérer rendre les intrusions rares, brèves et sans réel danger.

3.5 Conclusion

La sécurité réseau est un problème complexe. Pour sécuriser un site, il est nécessaire de connaitre les types d'attaques et les types d'agresseurs, ensuite prendre des précautions en adoptant par exemple une sécurité par l'obscurité ou sécurité par l'hôte ou autres techniques de sécurité.

CHAPITRE 4

ETUDE ET MIS EN PLACE D'UN RESEAU INTRANET

4.1 Etude du réseau intranet

4.1.1 Rappel sur le réseau Internet

L'Internet est le résultat de l'interconnexion de différents réseaux physiques en ajoutant des passerelles et en respectant certaines conventions. C'est un exemple d'interconnexion de systèmes ouverts. Dans le service Internet, le plus important se base sur un système de remise de paquets, non fiable et sans connexion. Le service est dit non fiable quand la remise n'est pas garantie. Un paquet peut être perdu, dupliqué, ou remis hors séquence mais l'Internet ne détectera rien et n'en informera ni l'émetteur ni le récepteur. Il est dit sans connexion lorsque chaque paquet est traité indépendamment des autres. Un envoi de paquets d'une machine à un autre peut utiliser des routes différentes : certains paquets se perdent et d'autres arriver à leur destination.

Pour le transfert du paquet, Internet utilise protocole TCP /IP .TCP/IP est un sigle très connu dans le domaine réseau. C'est un ensemble de deux protocoles : IP et TCP. [17]

Pour se communiquer à Internet, il faut des adresses. Ces adresses sont classées en trois catégories :

- Les adresses internet
- Les adresses IP
- Les adresses URL

- Les adresses Internet ou FQDN (Fully Qualifed Domain Name):

Les structures d'adresses étaient complexes à manipuler de par leur présentation en groupe de chiffres décimaux sous la forme abc : def : efg : hij : avec une valeur maximum de 255 pour chacun des quatre.

Les adresses IPv6 tiennent sur 8 groupes de quatre décimaux et l'entrée de telles adresses dans le corps d'un message deviendrait vite insupportable. C'est la raison pour laquelle l'adressage utilise une structure hiérarchique, beaucoup plus simple à manipuler et à mémoriser. Son format se présente généralement comme suit.

Format général : nom@organisation.domaine [17] [18]

Ou « nom » indique nom du serveur DNS, @ sépare nom du nom de domaine. L'organisation nationale ou internationale est une association des personnes qui visent des intérêts gouvernementales ou non gouvernementales, commerciales, éducatifs et abrégées par les préfixes suivantes :

.online,.linux,.fr,.etu, .org, .com, .microsoft, …….

Les serveurs de noms de « *DNS* »sont hiérarchiques et, lorsqu'il faut retrouver l'adresse IP d'un utilisateur, les DNS s'envoient des requêtes de façon à remonter suffisamment dans la hiérarchie pour trouver l'adresse IP correspondant. Ces requêtes sont effectuées par l'intermédiaire de petits messages qui portent la question et la réponse en retour.

- Les addresses URL (Uniform Resource Locator):

Une URL est un format de nommage universel pour désigner une ressource sur Internet. Une adresse URL est une adresse de la forme.

Service : //machine/répertoire/fichier

Il s'agit d'une chaîne de caractères ASCII imprimables qui se décompose en cinq parties:

- Le nom du protocole : c'est-à-dire le langage utilisé pour communiquer sur le réseau.
- L'Identifiant et le mot de passe : qui permettent de spécifier les paramètres d'accès à un serveur sécurisé. Cette option est déconseillée car le mot de passe est visible dans l'URL.
- Le nom du serveur : représente un nom de domaine dans l'ordinateur hébergeant la ressource demandée.
- Le numéro de port : décrit un numéro associé à un service qui permet au serveur de décrypter le type de ressource demandée.
- Le chemin d'accès à la ressource : Cette dernière partie permet au serveur de connaître l'emplacement auquel la ressource est située, c'est-à-dire de manière générale l'emplacement (répertoire) et le nom du fichier demandé. [17] [18]

- L'adresse logique où adresse IP :

L’adressage IP consiste à donner une adresse à chaque machine du réseau qui lui permet se localiser vis-à-vis de ce même réseau. Pour l’IPv4 cette adresse est formée par quatre octet séparé par des points du type : « x.y.z.t ». [17] [18]

4.1.2 Définitions de l’intranet

Définitions 4.01

Le mot intranet est devenu familier depuis une décennie bien qu’il renferme différentes interprétation. Un intranet est avant tout lié aux protocoles d’internet IP et TCP (ou UDP). Le paradigme intranet correspond au système d’information de l’entreprise utilisant les applicatifs de l’internet. Il désigne aussi parfois l’infrastructure de l’entreprise pour réaliser ses communications internes.

Un intranet est un ensemble de services internet interne à un réseau local, c'est-à-dire accessible uniquement à partir des postes d'un réseau local et invisible de l'extérieur. Il consiste à utiliser les standards client-serveur de l'internet (en utilisant les protocoles TCP/IP), comme par exemple l'utilisation de navigateurs internet, pour réaliser un système d'information interne à une organisation ou une entreprise. [7]

Un intranet repose généralement sur une architecture à trois niveaux, composée:

- du client (navigateur internet)
- du serveur d'application (middleware): un serveur web permettant d'interpréter des scripts CGI, PHP, ASP ou autres, et les traduire en requêtes SQL afin d'interroger
- une base de données d'un serveur de bases de données

De cette façon les machines clientes gèrent l'interface graphique, tandis que le serveur manipule les données. Le réseau permet de véhiculer les requêtes et les réponses. La figure suivante présente l’architecture client serveur à trois niveaux

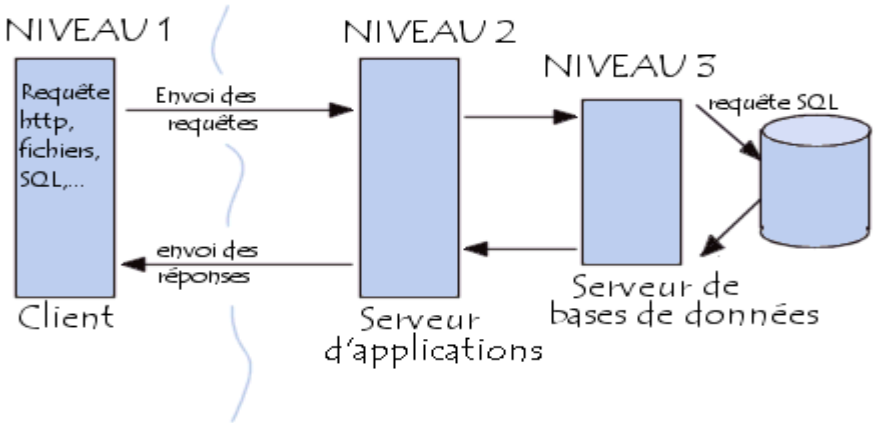

Figure 4.01 : *Architecture client serveur à trois niveaux*

La figure suivante permet d'avoir un aperçu de ce que c'est un intranet, composé de 8 machines clients et de quatre serveurs et avec 3 téléphones IP liées par un switch

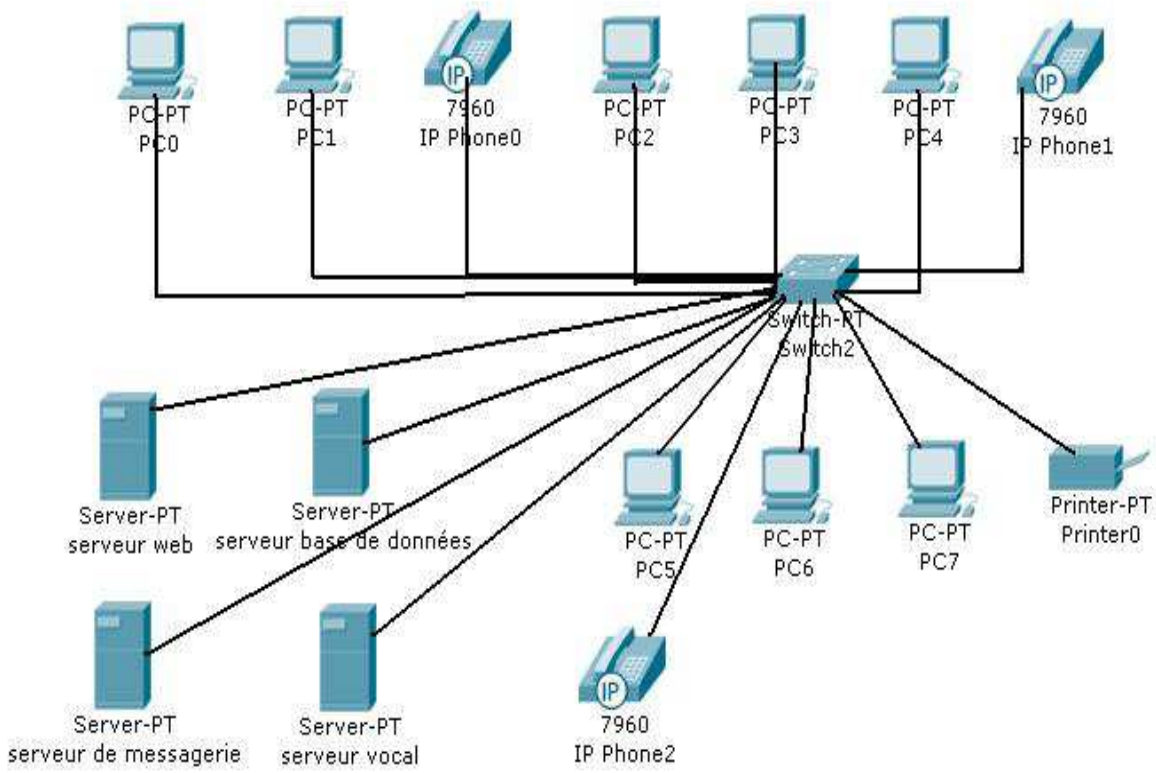

Figure 4.02 : *Intranet*

4.1.3 Objectifs et avantages de l'intranet

Lorsqu' on crée un intranet, les objectifs sont essentiellement de développer un système d'information à la taille de l'entreprise, auquel puissent accéder les personnels de l'entreprise et leurs clients, depuis n'importe quel point de l'entreprise, à n'importe quel moment et en utilisant une plate-forme quelconque. Cet environnement doit donc être indépendant de toute technologie propriétaire et permettre son utilisation pour le transfert d'informations, l'accès aux moyens de calcul et aux services, mais aussi pour la gestion du réseau et des services. L'intranet assure en outre une sécurité à un niveau à déterminer. [9]

Un intranet dans une entreprise permet de mettre facilement à la disposition des employés des documents divers et variés. Cela permet ainsi d'avoir un accès centralisé à la mémoire de l'entreprise. De cette façon, il est généralement nécessaire de définir des droits d'accès pour les utilisateurs de l'intranet, et par conséquent une authentification de ceux-ci afin de leur permettre un accès personnalisé à certains documents.

Des documents de tous types (textes, images, vidéos, sons, ...) peuvent être mis à disposition sur un intranet. De plus, un intranet peut réaliser une fonction de groupware très intéressante, c'est-à-dire permettre un travail coopératif par son intermédiaire. Voici quelques unes des fonctions qu'un intranet peut réaliser:

- Mise à disposition d'informations sur l'entreprise (panneau d'affichage)
- Mise à disposition de documents techniques
- Moteur de recherche de documentations
- Un système de gestion
- Un échange de données entre collaborateurs
- Annuaire du personnel
- Gestion de projets, aide à la décision, agenda, ingénierie assistée par ordinateur
- Messagerie électronique
- Forums de discussion, listes de diffusions, chat en direct
- Visioconférence
- Portail vers internet

De cette façon un intranet favorise la communication au sein de l'entreprise et limite les erreurs dues à la mauvaise circulation d'une information. L'information disponible sur l'intranet est mise à jour et évite les conflits de version.

Un intranet permet de constituer un système d'information à faible coût (concrètement le coût d'un intranet peut très bien se réduire au coût du matériel et de son entretien avec des postes clients fonctionnant avec des navigateurs gratuits, un serveur fonctionnant sous Linux avec le serveur web Apache et le serveur de bases de données MySQL).D'autre part, étant donné la nature "universelle" des moyens mis en jeu, n'importe quel type de machine peut être connecté au réseau local, donc à l'intranet.

4.1.4 Les outils nécessaires pour la réalisation de l'intranet

Pour mettre en place un intranet, on doit disposer des machines clients, des machines serveurs, des câbles pour la liaison filaire, des Switch ou routeur permettant de faire la liaison, des routeurs sans fils pour celui du sans fil. Il faut disposer aux moins les serveurs suivants :

- Un serveur de nom de domaine (DNS) permettant aux machines d'être reconnues par un nom en plus de leur adresse IP.
- Un serveur de messagerie qui donne la liberté aux clients d'envoyer et de recevoir des e-mails.
- Un serveur Web fournissant un site web interne.

- Un serveur de Gestion de bases de données permettant d'administrer une base de données.
- Un serveur de fichiers afin de permettre aux utilisateurs de l'intranet d'accéder à un ensemble de fichiers partagés
- Un serveur d'impression
- Un serveur LDAP
- Un serveur de commande à distance

Dans notre cas on va utiliser linux comme serveur, alors La machine sur laquelle sera installé Linux proposera l'ensemble des services suivants :

- Un serveur de nom de domaine (DNS) permettant aux machines d'être reconnues à l'aide d'un nom. Dans notre cas, on supposera que l'adresse IP du serveur est 192.168.10.6
- Un serveur de messagerie permettant aux clients d'envoyer et de recevoir des e-mails. Le serveur de messagerie le plus répandu est SendMail, mais étant donné la complexité de sa configuration, nous utiliserons postfix. Celui-ci permettra l'utilisation de SMTP (courrier sortant) et POP (courrier entrant)
- Un serveur Web fournissant un site web interne. Le serveur utilisé sera Apache2 (le serveur le plus utilisé au monde) avec le support du langage PHP pour permettre l'utilisation de pages dynamiques
- Un serveur de bases de données (SGBD) permettant d'administrer une base de données. Nous installerons MySQL, un SGBD gratuit fonctionnant sous Linux
- Un serveur de fichiers afin de permettre aux utilisateurs de l'intranet d'accéder à un ensemble de fichiers partagés. Nous utiliserons SAMBA qui a l'avantage d'être entièrement compatible avec les réseaux Microsoft
- Un serveur LDAP fournissant un service d'annuaire très puissant.
- Une liste de diffusion pour autoriser les utilisateurs à envoyer un courrier à l'ensemble (ou une partie) des utilisateurs de l'intranet

4.2 Les applications de l'intranet

Intranet a démarré avec des applications simples, comme le courrier électronique et le transfert de fichiers, pour offrir aujourd'hui de services extrêmement complexes dans les quels on peut naviguer pour rechercher une information souhaitée.

Les applications les plus classiques d'Intranet comprennent la messagerie électronique SMTP, le transfert des fichiers FTP, le terminal virtuel Telnet, l'accès aux pages de fichiers distribués NFS, et les applications liées au Web

4.2.1 Courrier électronique

- Généralités sur le courrier ´électronique :

Le courrier électronique, ou *"mail"* est l'un des deux services les plus populaires, avec le web. C'est aussi l'un des plus vieux services du réseau, bien avant les évolutions actuelles que l'on peut apprécier. [9]

- Le protocole SMTP :

SMTP, l'une des premières applications Internet qui représente une messagerie électronique relativement simple. Cette application se sert des adresses définies dans l'Internet du type nom@entreprise.domain ou la deuxième partie représente le nom du domaine qui gère le serveur de messagerie. [9]

La syntaxe utilisée dans la messagerie Internet est également très simple : un en-tête comportant quelques éléments de bases, comme l'objet du message, l'émetteur, le récepteur, la date et le corps du message. Le tout en ASCII.

4.2.2 Serveur de noms – DNS

- Généralités sur le serveur de noms :

Il traduit l'adresse IP en nom. Ce nommage symbolique est simplement beaucoup plus naturel pour les Humains que la manipulation des adresses IP, même sous forme décimale pointée.

Il n'intervient donc qu'au niveau applicatif, ainsi la majeure partie des applications réseaux font usage de noms symboliques avec, de manière sous-jacente, une référence implicite à leur(s) correspondant (s) numérique(s).[9] [19]

- Fonctionnement du DNS :

Précisons que les noms de machines sont développés un peu comme les noms de fichiers d'un système hiérarchisé (Unix,. . .).

  - Le ". " est le séparateur
  - Chaque nœud ne peut faire que 63 caractères au maximum ; " le bon usage " les limite en 12 caractères et commençant par une lettre.

- Les majuscules et minuscules sont indifférenciées.
- Les chiffres [0-9] et le tiret peuvent être utilisées, le souligné ( ) est un abus d'usage.
- Le point ". " et le blanc " " sont prescrits.
- Les chaînes de caractères comme " NIC " ou d'autres acronymes bien connus sont à éviter absolument, même encadrées par d'autres caractères.
- Les noms complets ne doivent pas faire plus de 255 caractères de long. [9] [19]

4.2.3 FTP

- Définition :

FTP est un protocole de transfert de fichiers qui permet de garantir une qualité de service. Ce transfert de fichiers s'effectue entre deux adresses extrémités du réseau Internet.

L'application FTP est du type client-serveur avec un utilisateur FTP et un serveur FTP. Dans le cas de FTP anonyme, il faut se connecter sous un compte spécial et, selon la convention, donner son adresse de messagerie électronique comme mot de passe. [9]

- Le rôle du protocole FTP :

Le protocole FTP définit la façon selon laquelle des données doivent être transférées sur un réseau TCP/IP. FTP met en place une session temporaire dans le but de transférer un ou plusieurs fichiers. Le transfert a lieu par intermédiaire du logiciel client, auquel on donne l'adresse de la machine FTP sur laquelle on souhaite récupérer les fichiers. Une fois le transport effectué, la session est fermée

- Objectifs du FTP :

  - permettre un partage de fichiers entre machines distantes
  - permettre une indépendance aux systèmes de fichiers des machines clientes et serveur
  - permettre de transférer des données de manière efficace

- Le modèle FTP :

Le protocole FTP s'inscrit dans un modèle client-serveur, c'est-à-dire qu'une machine envoie des ordres (le client) et que l'autre attend des requêtes pour effectuer des actions (le serveur). [9]

Lors d'une connexion FTP, deux canaux de transmission sont ouverts :

- Un canal pour les commandes (canal de contrôle)
- Un canal pour les données

4.2.4 Telnet

Telnet est une application de connexion à distance, qui permet de connecter un terminal sur une machine distante. C'est l'application de terminal virtuel.

La connexion Telnet utilise le protocole TCP pour transporter les informations de contrôle nécessaire à l'émulation de la syntaxe du terminal. Dans la plupart des cas, Telnet est utilisé pour établir une connexion entre deux machines en communication de négocier des options entre elles par des ensembles préétablis. [9]

Le protocole Telnet repose sur trois concepts fondamentaux :

- Le modèle du terminal réseau virtuel (*Network Virtual Terminal*)
- Le principe d'options négociées
- Les règles de négociation

Lorsque le protocole Telnet est utilisé pour connecter un hôte distant à la machine sur lequel il est implémenté en tant que serveur, ce protocole est assigné au port 23.

4.2.5 Usenet News

Les Usenet news correspondent à des forums d'utilisateurs ayant en commun un sujet de discussion. Chaque utilisateur du groupe peut ajouter ses propres documents sous forme de fichiers ASCII. Le forum possède une liste d'utilisateurs, lesquels sont libres de supprimer leur nom ou d'ajouter lorsqu'ils le veulent. Ceci est une application Internet mais on peut l'utiliser comme application intranet surtout pour ce qui utilise Intranet à des longues distances (exemple : à des différents immeubles, différents zones). [9] [19]

4.2.6 WWW

- Généralité :

Le WWW est un système de documents hypermédia distribué, qui a été crée par Tim Berners-Lee en 1989.

Ce système fonctionne en mode client-serveur ; les logiciels clients, encore appelés navigateurs Web (Mosaic, Netscape, Microsoft Explorer, Mozila Firefox) , utilisent le protocole de communication http pour accéder, via le réseau Internet, aux documents hébergés sur un serveur

Web distant. Ces documents sont représentés à l'aide d'un langage de description de pages, HTML.

Ce dernier définit la manière dont les différents éléments des documents (titres, tableaux, …) seront représentés sur l'écran du poste client et de relier les documents entre eux, quels que soit leur localisation géographique, en créant des liens logiques, appelés liens hypertexte.

Ces liens sont indiqués visuellement sur la page écran et un simple clic dessus permet de se connecter au site possédant l'information sous-jacente. L'ensemble de tous ces liens entre documents est assimilé à une toile d'araignée, d'où le nom de Web. [9] [19]

Les services web (en anglais web services) représentent un mécanisme de communication entre applications distantes à travers le réseau Internet indépendant de tout langage de programmation et de toute plate-forme d'exécution :

- utilisant le protocole HTTP comme moyen de transport. Ainsi, les communications s'effectuent sur un support universel, maîtrisé et généralement non filtré par les pare-feux
- employant une syntaxe basée sur la notation XML pour décrire les appels de fonctions distantes et les données échangées
- organisant les mécanismes d'appel et de réponse.

Communication entre navigateur et serveur :
La communication entre le navigateur et le serveur se fait en deux temps :

- Le navigateur effectue une requête HTTP
- Le serveur traite la requête puis envoie une réponse HTTP.

4.2.7 Le service DHCP

DHCP ou adressage IP automatique. Il s'agit d'un protocole qui permet à un ordinateur connecté à un réseau, d'obtenir dynamiquement (c'est-à-dire sans intervention particulière) sa configuration (principalement, sa configuration réseau). On n'a qu'à spécifier à l'ordinateur de se trouver une adresse IP tout seul par DHCP. Le but principal de ce protocole est de simplifier l'administration d'un réseau.

Le protocole DHCP sert principalement à distribuer des adresses IP sur un réseau, mais il a été conçu au départ comme complément au protocole BOOTP utilisé lors de l'installation d'une machine, par exemple, à travers un réseau (BOOTP est utilisé en étroite collaboration avec un

serveur TFTP sur lequel le client va trouver les fichiers à charger et à copier sur le disque dur). Un serveur DHCP peut renvoyer des paramètres BOOTP ou de configuration propres à un hôte donné. [9]

4.2.8 NFS

NFS a pour fonction d'assurer un accès transparent à des ressources distantes sur un réseau, en donnant l'impression à l'utilisateur que ces ressources sont locales, et ce quels que soient les réseaux et protocoles utilisés de manière sous-jacente. De ce fait NFS ne désigne pas à proprement parler une application spécifique d'Internet mais une application plus générale, qui pourrait se concevoir sur tout type de système distribué. [9]

4.2.9 WAIS

WAIS est un système de type client-serveur, qui permet d'effectuer des recherches dans la base de données distribuées. [9]

4.3 Mis en place du réseau intranet

4.3.1 Adressages des machines et câblages

4.3.1.1 Répartitions des salles et des machines

1er cas : les ordinateurs se trouvent dans un même bâtiment

Supposons que notre entreprise possède quatre salles dont :

La salle N°01 contient 4 ordinateurs

La salle N°02 contient 4 ordinateurs

La salle N°03 contient 3 ordinateurs

La salle N°04. Sur cette salle on va mettre les serveurs

Illustrons à l'aide d'une figure cette répartition des salles et des machines

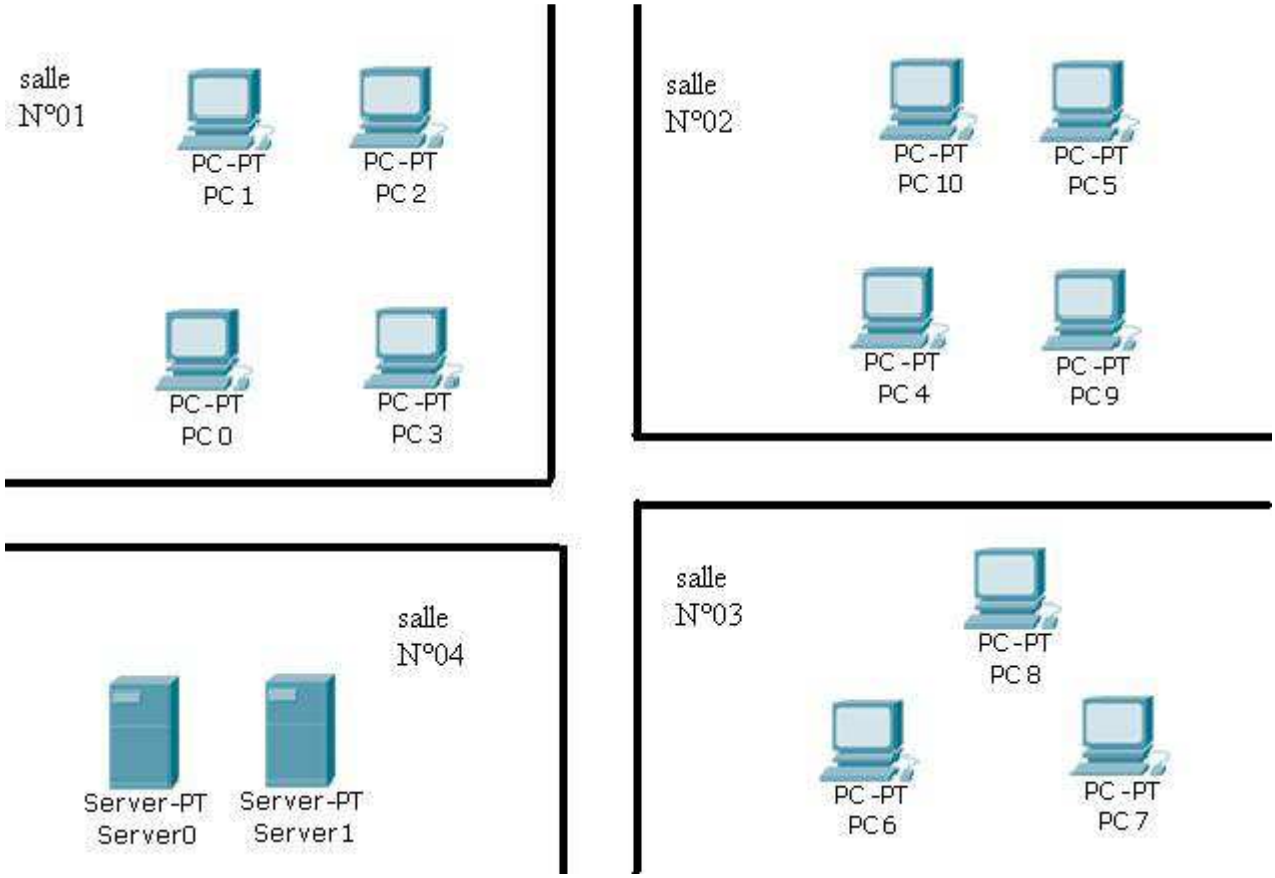

Figure 4.03 : *Répartition des salles et des ordinateurs*

Pour mettre en place un réseau Intranet au sein d'une entreprise, il faut commencer par analyser les paramètres essentiels qui déterminent la performance d'une machine. C'est-à-dire :

- Ses configurations de base
- Le système d'exploitation installé sur chaque machine
- Quelles sont les cartes installées sur la machine y compris la carte réseau

2eme cas : on a deux sites dans des immeubles différents

Supposons que dans le premier immeuble (notons immeuble A) possède quatre salles dont :

Salle N°01 : contient quatre ordinateurs

Salle N°02 : contient trois ordinateurs

Salle N°03 : contient un seul ordinateur

Salle N°04 : salle où on va mettre deux serveurs

Supposons que dans le second immeuble (notons immeuble B), on a trois salles dont

La salle N°01 : salle où on va mettre un serveur

La salle N°02 : contient trois ordinateurs

La salle N°03 : contient deux ordinateurs

La liaison entre les deux bâtiments est assurée par : des câbles coaxiaux, des fibres optiques ou par accès sans fil. Illustrons à l'aide d'une figure ces répartitions :

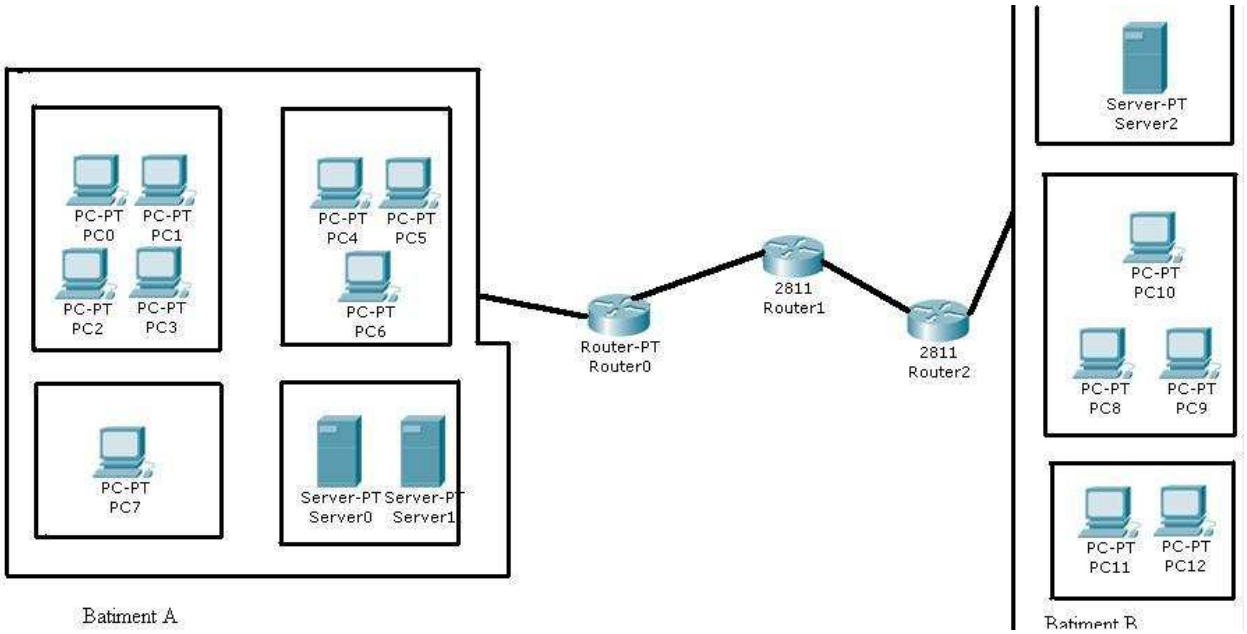

Figure 4.04: *répartition des machines dans des bâtiments différents*

Maintenant, il faut analyser les performances des machines en déterminant :

- Ses configurations de base
- Le système d'exploitation installé sur chaque machine
- Quel est la carte réseau sur chaque machine

4.3.1.2 Adressages et câblages des machines

Après la répartition des machines et des salles, maintenant on va passer à l'adressage de chaque machine. Il existe deux moyens pour faire l'adressage IP de chaque machine :

En configurant l'adresse IP de chaque machine (même pour le serveur): dans notre cas, comme c'est un réseau privé, on va mettre 192.168.10 pour l'adresse réseau et de .2 jusqu'à .50 pour l'hôte.

En utilisant DHCP, qui configure automatiquement l'adresse tout en mettant l'utilisateur à 50 et l'adresse de départ à 192.168.10.1.

Pour le câblage, on va utiliser le RJ 45 avec le câble à paire torsadée pour la liaison locale c'est-à-dire tout ce qui se trouve sur le même bâtiment, et des câbles coaxiaux, des fibres optiques, ou sans fils pour la liaison entre des bâtiments différents. Lorsqu'on finit le câblage et l'adressage, on peut tester la connexion en utilisant la commande Ping. Après cela on va installer et configurer le serveur.

4.3.2 Installation et configuration du serveur

4.3.2.1 Installation et configuration du DNS

On va installer Bind9 comme serveur DNS, pour cela

apt –get install DNS

Les fichiers de configuration de Bind se trouvent dans le répertoire /etc/bind/. On y trouve notamment le fichier db.root, qui contient les adresses IP des serveurs DNS racines, et le fichier named.conf qui est le fichier de configuration principal de Bind. Le répertoire /var/cache/bind/ est destiné à accueillir les fichiers de zone pour ceux qui veulent configurer un serveur DNS primaire ou secondaire. Pour la configuration du DNS, on va ajouter à la fin du fichier named.conf les lignes suivantes.

```
zone "entreprise.mg" {
type master;
file "entreprise.mg.zone";
};
```

Où :

- entreprise.mg est le nom de domaine pour lequel le serveur sera primaire,
- entreprise.mg.zone désigne le fichier /var/cache/bind/mondomaine.org.zone où seront stockés les enregistrements de la zone.

On copie les configurations dans le db.local vers db.entreprise.mg pour avoir quelques syntaxes

cp db.local db.entreprise.mg

Maintenant il faut vérifier la syntaxe si on a fait des erreurs pendant l'édition, pour cela on utilise la commande check

name – checkconf /etc/bind9/named.conf

name - checkzone entreprise.mg db.entreprise.mg

Si la commande n'affiche aucun message d'erreur, alors il n'y a pas d'erreur de syntaxe dans le fichier de zone. On peut alors dire à Bind de relire son fichier de configuration :
/etc/init.d/bind9 reload

Pour tester le serveur DNS, L'utilitaire dig permet de faire des requêtes DNS évoluées et fournit un maximum d'informations sur la requête. Il est très utile pour vérifier la bonne configuration d'un serveur DNS.

4.3.2.2 Installation et configuration du serveur web

Apache est un des serveurs web les plus utilisés dans le monde. Dans notre cas on va utiliser la version 2, pour l'installer :
apt-get install apache2

Les fichiers de configuration d'Apache sont dans le répertoire /etc/apache/. Pour pouvoir mettre une page web à disposition du monde, on va éditez le fichier /etc/apache/httpd.conf, décommentez la ligne 309 et mettez le nom DNS de notre machine :
ServerName entreprise.mg

Si on veut mettre des restrictions d'accès aux pages avec des fichiers .htaccess, , on modifiera également la ligne 357 en écrivant :
AllowOverride All

Maintenant que la configuration a été modifiée, il faut dire à Apache de relire ses fichiers de configuration :
/etc/init.d/apache reload
Reloading apache configuration.

Maintenant on va ajouter le support PHP, s'il est déjà installé alors on laisse sinon
apt-get install php4
Pendant l'installation, il demande quelques configurations
Ensuite, on va éditer le fichier /etc/apache2/httpd.conf :

- pour dire à Apache de charger le module PHP, on va décommenter la ligne suivante :

LoadModule php4_module /usr/lib/apache/1.3/libphp4.so

- pour dire à Apache de faire passer par l'interpréteur PHP toutes les pages d'extension .php, on va décommentez la ligne suivante :

    AddType application/x-httpd-php .php

Enfin, dites à Apache de relire son fichier de configuration :

/etc/init.d/apache reload

Reloading apache configuration.

Toutes les pages ayant l'extension .php seront désormais traitées par l'interpréteur PHP avant d'être envoyées par Apache au navigateur Web distant.

La page web à mettre à disposition du monde doit se trouver dans le répertoire /var/www/, s'appeler index.html et avoir les droits en lecture pour tout le monde. Une page Web a été mise par défaut à l'installation d'Apache. Cette page web est maintenant disponible à l'adresse **http://www.entreprise.mg** pour le monde entier.

Les utilisateurs du système peuvent également mettre leur page Web à disposition du monde. Par exemple, pour l'utilisateur jack, il suffit qu'il crée un répertoire public_html dans son home avec un fichier index.html dedans. Les permissions doivent être au minimum les suivantes :

% chmod 711 /home/jack/

% chmod 711 /home/jack/public_html/

% chmod 644 /home/jack/public_html/index.html

La page web de jack est désormais disponible au monde entier à l'adresse http://www.entreprise.mg/~jack/

4.3.2.3 Installation et configuration du serveur mail

On va installer postfix comme serveur mail

apt –get install postfix

La configuration de Postfix se fait dans le fichier /etc/postfix/main.cf .

Une fois qu'on personnalisé le fichier main.cf en lisant les commentaires contenus dans le fichier, il faut dire à Postfix de relire sa configuration :

/etc/init.d/postfix reload

Les utilisateurs qui ont des comptes sur le serveur peuvent alors recevoir du mail à l'adresse nom_du_compte@nom_de_domaine. Le mail reçu pour l'utilisateur jack est stocké dans le fichier /var/mail/jack

Pour gérer les mails entrants et / ou sortants on va installer Imap et /ou POP

Pour installer un serveur POP, il suffit d'installer qpopper

apt-get install qpopper

La configuration de qpopper se fait dans le fichier /etc/qpopper.conf. Par défaut, tout est commenté, mais les paramètres par défaut doivent permettre de l'utiliser normalement.

Pour installer Imap, on a le package uw – imapd

apt-get install uw-imapd

Ceci n'a pas de fichier de configuration

Maintenant on va installer squirrelmail pour controler le mail via un navigateur web, pour sa configuration on va copier la syntaxe d'apache.conf à squirrelmail.conf

cp apache.conf /etc/apache2.conf/squirrelmail.conf

Maintenant, on va recharger apache2

/etc/init.d/apache2 reload

4.3.2.4 Installation du phpbb

Phpbb est utilisé pour faire une discussion en ligne ou forum. Pour son installation il faut le tarer puis installer

Dkpg phpbb.6.3

Et suivre ce qui est se trouve dans l'aide de l'installation.

4.3.2.5 Installation et configuration du serveur FTP

Un des serveurs FTP les plus utilisés est ProFTPd . Pour l'installer :

apt-get install proftpd

Dès l'installation, il pose des questions de configuration :

Modifier le fichier de configuration /etc/proftpd.conf ? Répond Oui.

Lancer ProFTPd à partir d'inetd ou indépendamment ? Répond indépendamment.

Autoriser les connexions anonymes ? Les connexions anonymes sont des connexions sans authentification qui permettent à n'importe qui de venir se connecter par FTP et de télécharger les fichiers qui se trouvent dans le home de l'utilisateur ftp (par défaut, c'est le répertoire /home/ftp/). Si on veut mettre en place un tel service, répond Oui.

Si on a répondu *Oui* à la question précédente, il vous demande Do you want /etc/proftpd.conf to be updated ?

Répond Oui.

Le serveur FTP est maintenant lancé. On peut modifier sa configuration en éditant le fichier /etc/proftpd.conf et avec l'aide qui se trouve dans la documentation disponible dans le package proftpd-doc. A chaque fois que le fichier de configuration change, il faut dire à ProFTPd de relire ses fichiers de configuration avec la commande :

/etc/init.d/proftpd reload

Les personnes qui ont un compte sur le système peuvent désormais se connecter par FTP avec leur login et leur mot de passe. Ils peuvent télécharger et déposer des fichiers dans tous les répertoires sur lesquels ils ont les droits nécessaires.

4.3.3 Résultat et Test

4.3.3.1 Test du serveur DNS

Un personnel va accéder au serveur à l'aide du nom du domaine, pour cela il va taper l'adresse www.entreprise.mg. Après cela, une page d'authentification l'attend, ceci est nécessaire pour une degré de sécurité, donc l'employé doit connaitre le login et le mot de passe du site. Cette page d'authentification se présente comme suit

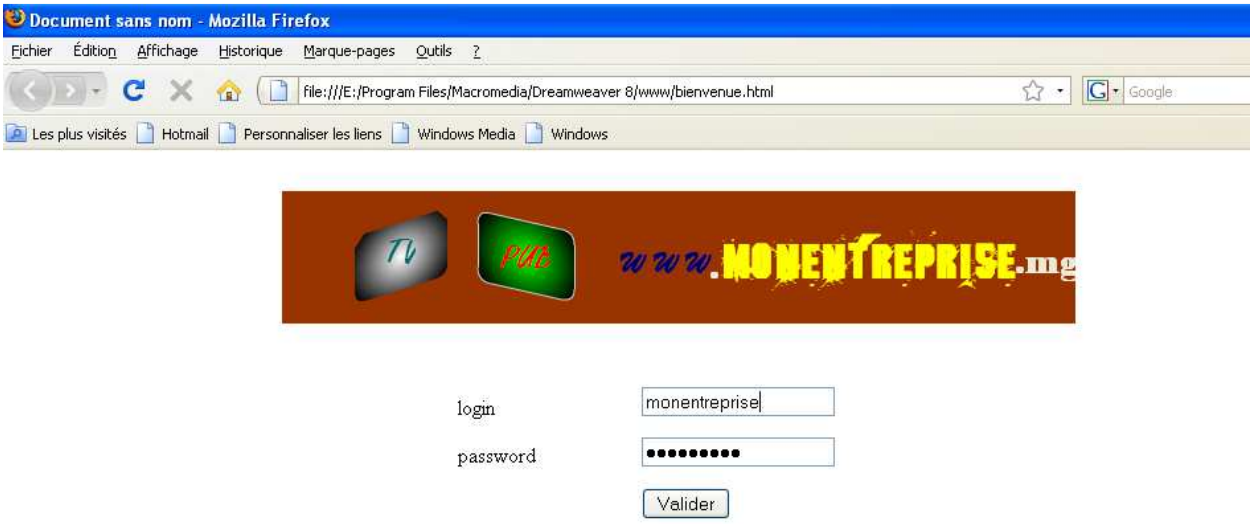

Figure 4.05 : *Page d'authentification*

Si ce personnel arrive à s'authentifier, une page qui contient un moteur de recherche l'attend. Ce moteur de recherche est nécessaire pour rechercher des documents, des informations mais seulement dans l'entreprise, il est aussi nécessaire surtout pour le nouvel personnel qui ne connait pas encore le nom du site alors il peut rechercher via ce moteur de recherche. Cette page est illustrée par la figure suivante

Figure 4.06 : *page contenant le moteur de recherche*

Si un personnel ne connait pas le nom du site, il peut taper sur le champ du texte le mot contenant « monentreprise » et le moteur de recherche va indexer touts les mots contenant « monentreprise ».

La figure suivante permet de visualiser cet index

Figure 4.07 : *Index*

Maintenant le personnel peut accéder au site de l'entreprise grâce au lien qui se trouve en haut « accéder au site de l'entreprise » et peut avoir les différentes services fournit par l'intranet. La figure suivante permet de montrer ce site

Figure 4.08 : *site de l'entreprise*

4.3.3.2 Test du serveur de base de données

En cliquant le lien « Gérer les bases de données », on peut gérer les bases de données de l'entreprise. Ceci est plutôt réservé aux administrateurs de la base de données parce qu'il nécessite la connaissance du commande SQL. La figure suivante permet de voir l'interface permettant de s'authentifier avant d'entamer la gestion de la base de données

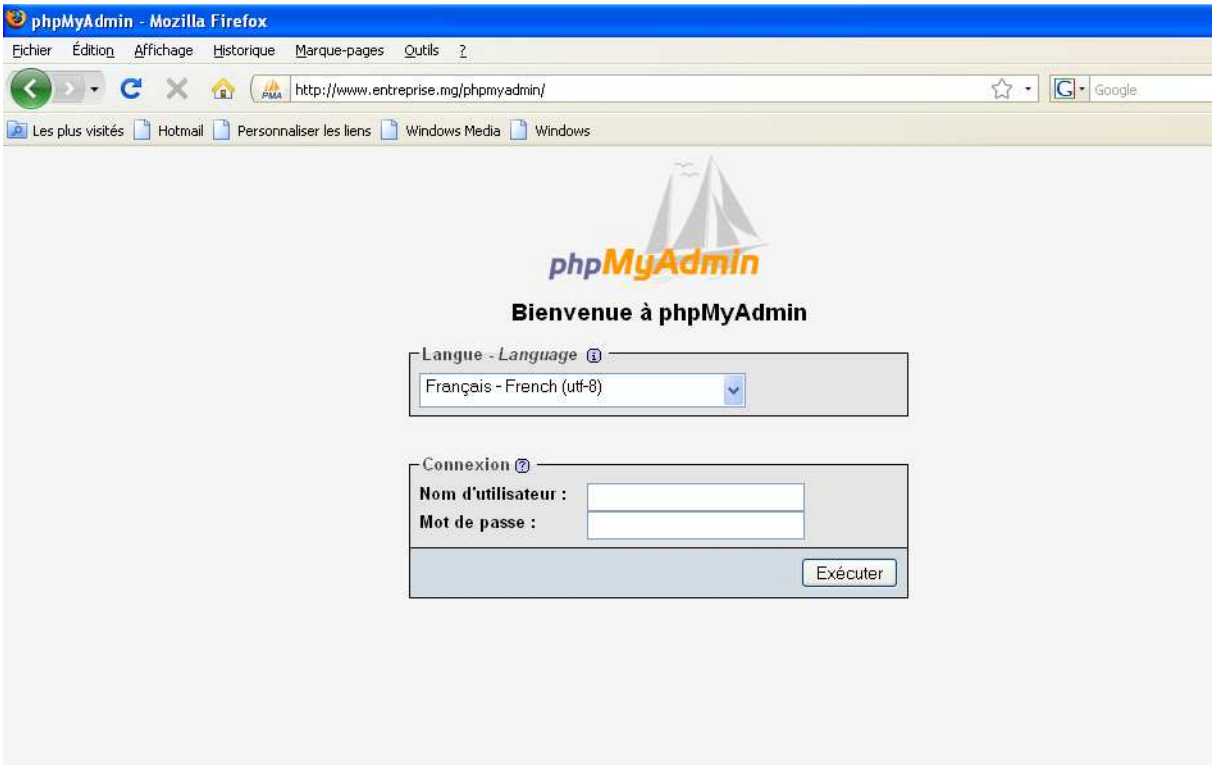

Figure 4.09 *: interface d'authentification*

Si l'utilisateur arrive à s'authentifier alors, il peut gérer la base de données via l'interface suivante

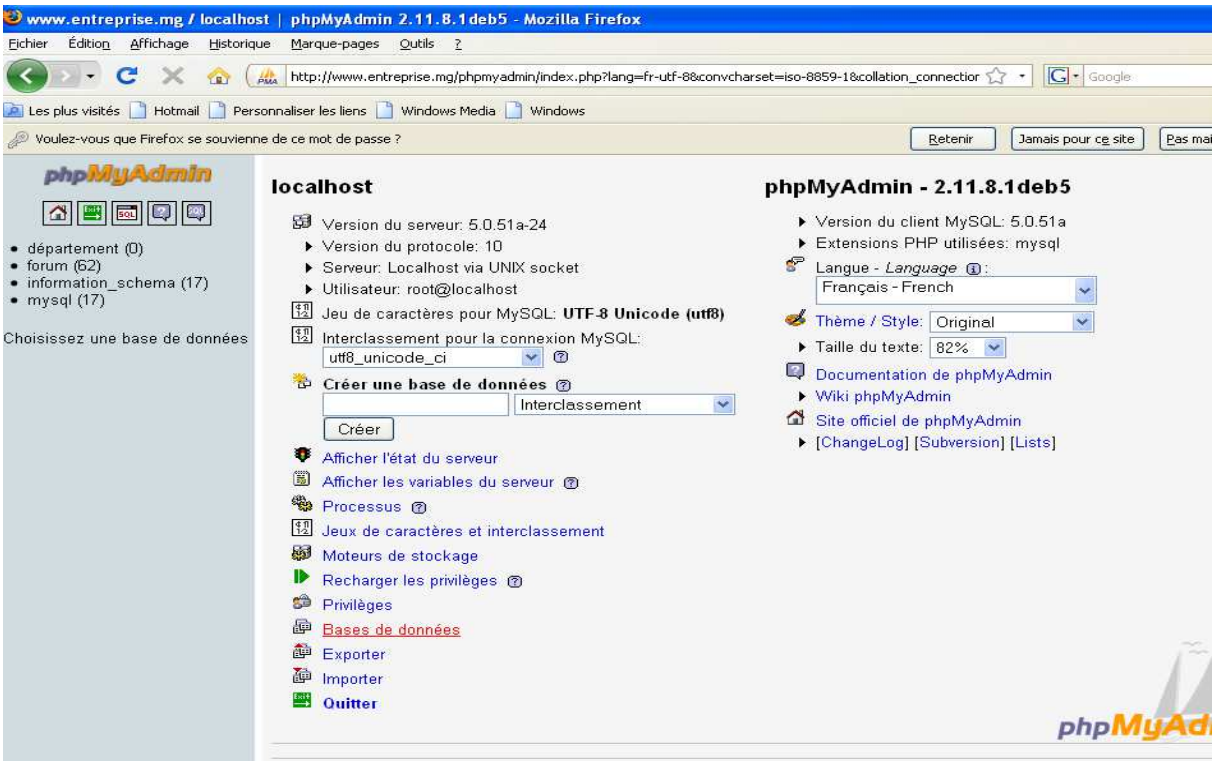

Figure 4.10 : *Interface permettant de gérer les bases de données*

4.3.3.3 Test du serveur Mail

Si le personnel veut consulter ou envoyer des mails, il va cliquer le lien « envoyer des courriers », après cela une interface permettant d'identifier l'utilisateur va ouvrir. La figure suivante montre cette interface

Figure 4.11 : *interface d'authentification pour le mail*

Si l'utilisateur arrive à s'authentifier, il peut accéder aux mails par l'interface suivante

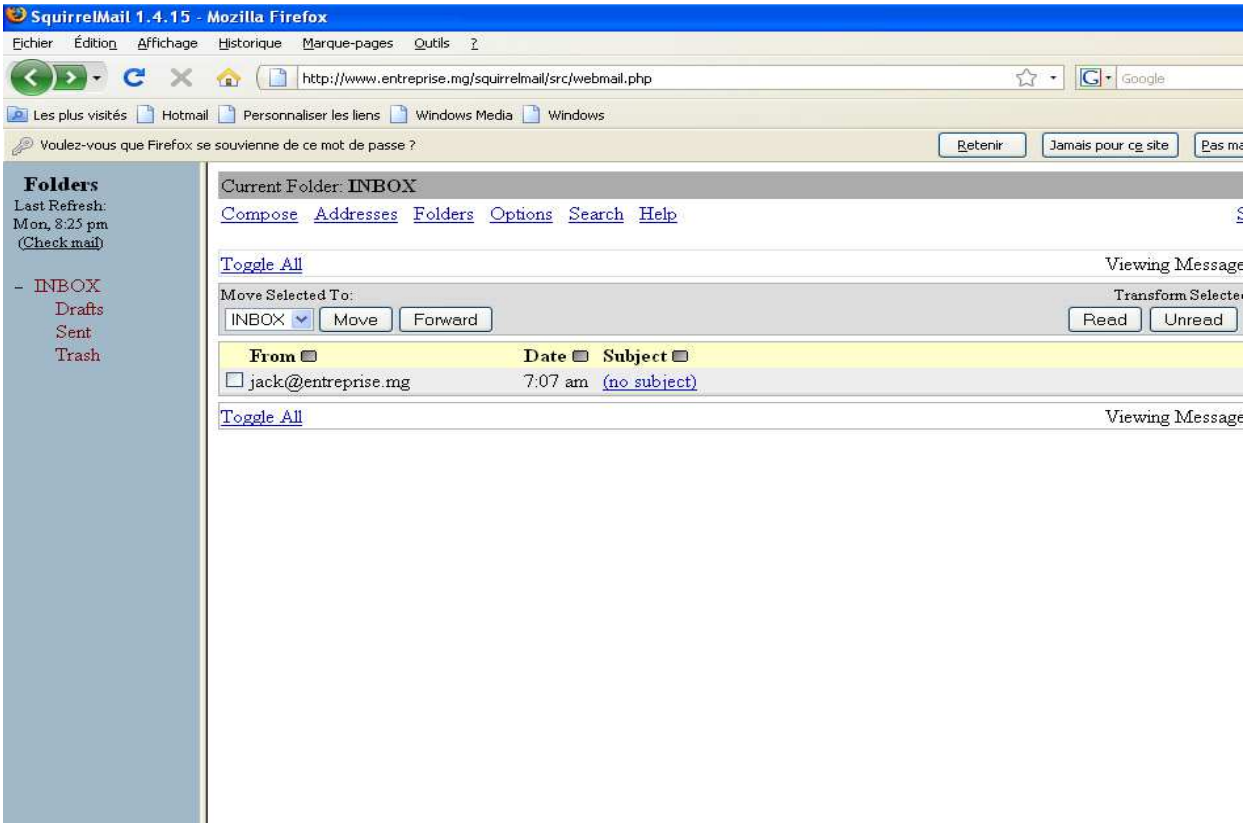

Figure 4.12 : *interface permettant d'accéder aux mails*

Si l'utilisateur veut voir les mails, il suffit de cliquer sur le lien contenant le sujet. S'il veut envoyer, on clique sur le lien « compose » et une interface permettant d'envoyer les mails se présente

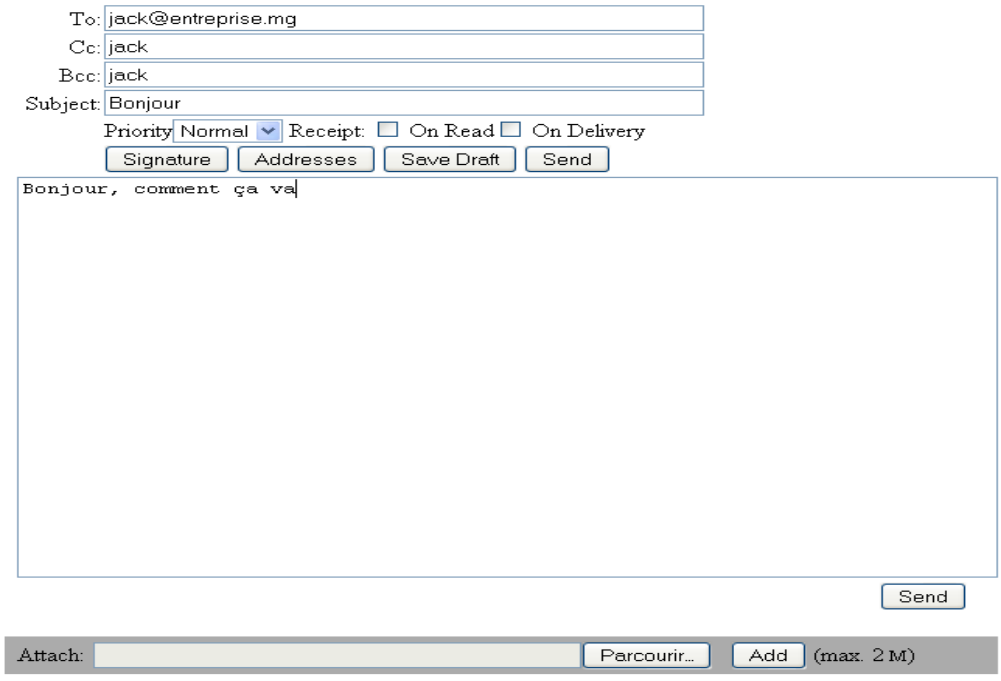

Figure 4.13 : *interface permettant d'envoyer des mails*

4.3.3.4 Test du serveur FTP

Le personnel peut télécharger des fichiers, ou des documents de l'entreprise en cliquant le lien « télécharger des fichiers ». La figure suivante présente cette interface de téléchargement

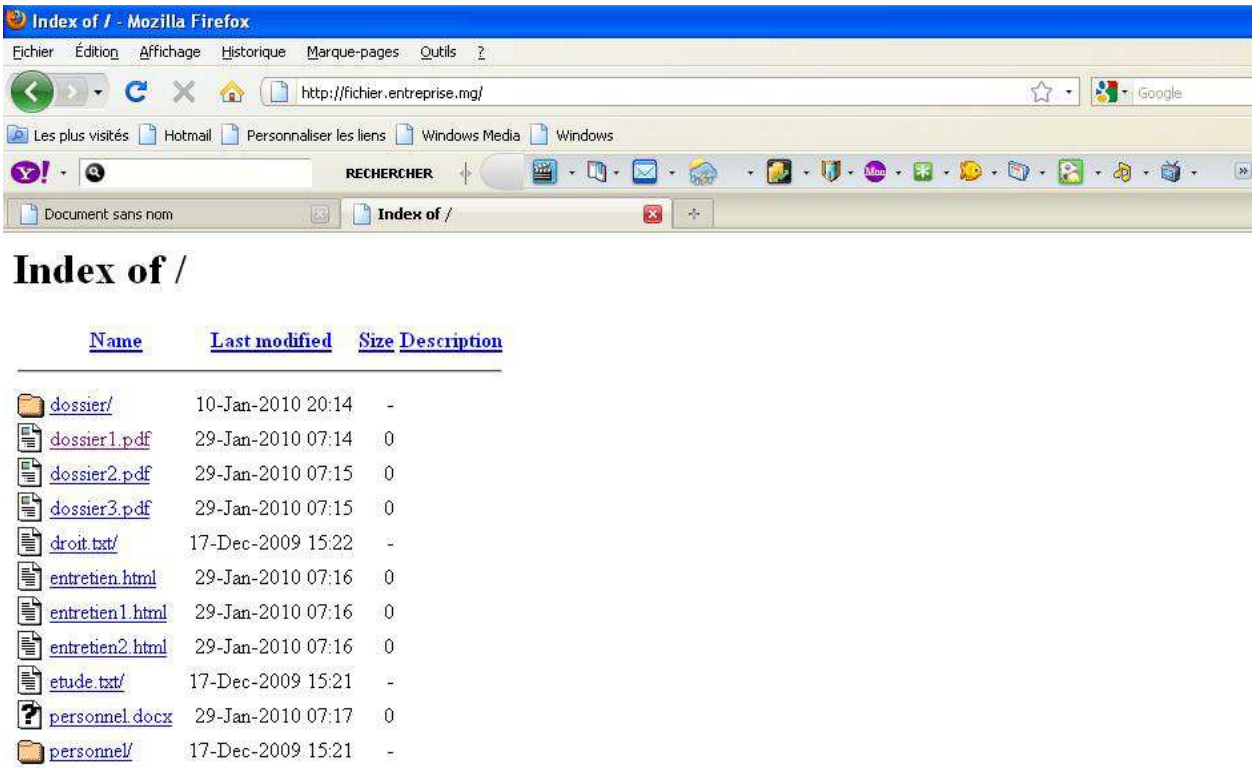

Figure 4.14 : *Interface contenant les fichiers à télécharger*

Pour télécharger les fichiers, on fait une clique droite sur les éléments à télécharger et on enregistre le lien sous un autre fichier comme le montre la figure suivante

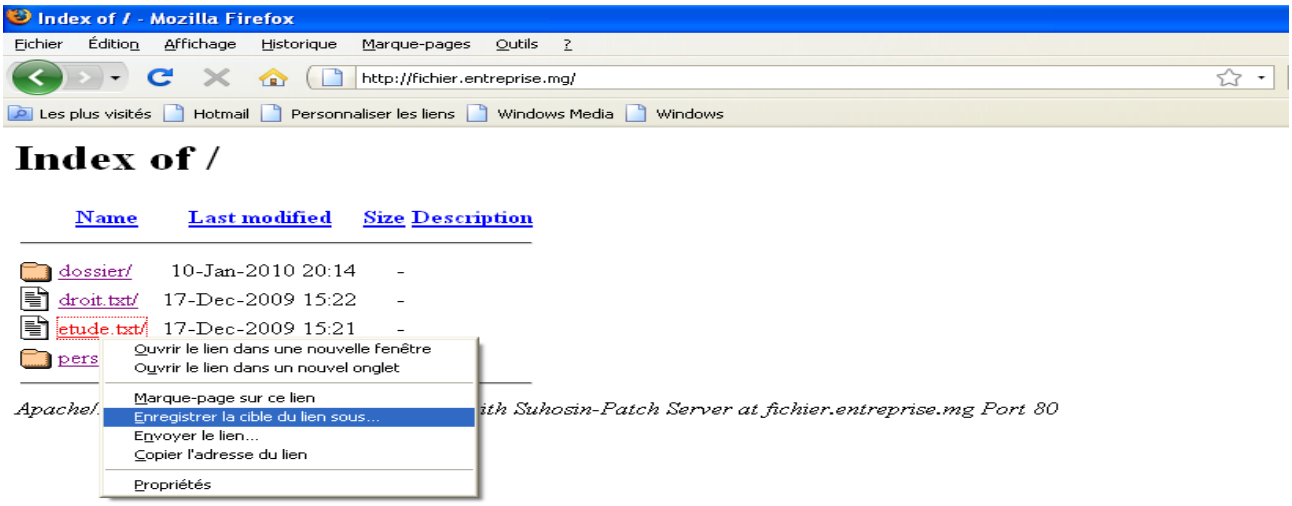

Figure 4.15 : *téléchargement des fichiers*

4.3.3.5 Forum

Pour faire un forum, l'utilisateur va cliquer le lien « faire des discussions », après cela une interface permettant de s'authentifier se présente. Si c'est la première fois qu'on fait une discussion, une interface d'enregistrement se présente. La figure suivante montre un aperçu de ce forum

Figure 4.16 : *forums*

Et pour le gestionnaire d'annuaire, on clique sur le lien gestionnaire d'annuaire et on une interface comme suit :

Figure 4.17 : *gestionnaire d'annuaire LDAP*

Le gestionnaire d'annuaire est nécessaire pour centraliser les informations. Pour entrer dans l'interface on clique sur login pour s'authentifier et on a l'interface suivant :

Figure 4.18 : *interface pour enregistrer les informations*

CHAPITRE 5

ETUDE ET REALISATION DU FIREWALL INTERNET

5.1 Introduction

Chaque ordinateur connecté à internet (et d'une manière plus générale à n'importe quel réseau informatique) est susceptible d'être victime d'une attaque d'un pirate informatique. La méthodologie généralement employée par le pirate informatique consiste à scruter le réseau en envoyant des paquets de données de manière aléatoire à la recherche d'une machine connectée, puis à chercher une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant.

Cette menace est d'autant plus grande que la machine est connectée en permanence à internet pour plusieurs raisons :

- La machine cible est susceptible d'être connectée sans pour autant être surveillée ;
- La machine cible est généralement connectée avec une plus large bande passante ;
- La machine cible ne change pas (ou peu) d'adresse IP.

Ainsi, il est nécessaire, autant pour les réseaux d'entreprises que pour les internautes possédant une connexion de type câble ou ADSL, de se protéger des intrusions réseaux en installant un dispositif de protection. Un de ces dispositifs est le firewall.

5.2 Définitions

Définition 5.01

Le mot firewall possède plusieurs traduction en français : pare-feu et garde barrière étant les deux plus classique. Pour cette étude on va garder le mot firewall.

Un firewall est un routeur spécifique qui se trouve à l'entrée d'une entreprise et dont le but est d'empêcher l'entrée ou la sortie des paquets non autorisés par l'entreprise. [7]

Un firewall permet de contrôler l'entrée et la sortie des données grâce entre autres à l'ouverture/fermeture des ports, Il filtre les paquets de données entrantes et/ou sortantes. [9]

La situation géographique d'un firewall est illustrée par la figure suivante :

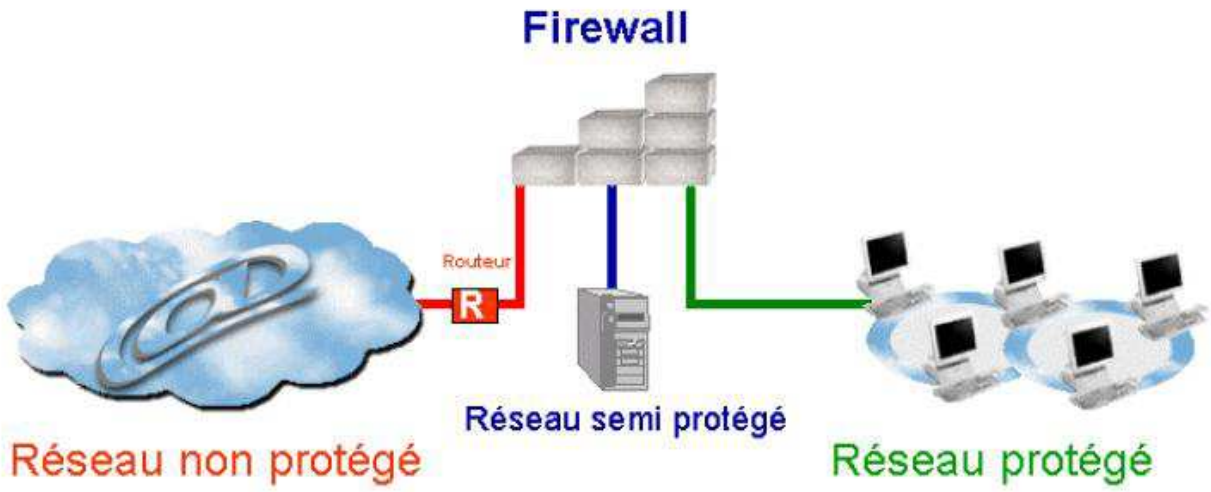

Figure 5.01 : *Situation d'un firewall dans une entreprise*

En théorie un firewall internet sert à empêcher les dangers provenant de l'internet de se répandre à l'intérieur d'un réseau. Il sert à plusieurs choses :

- Restreint l'accès à un point précis
- Empêche les agresseurs de s'approcher des autres défenses.
- Restreint la sortie à un point précis

Tout le trafic provenant de l'internet ou partant du réseau interne passe à travers le firewall, qui a donc la possibilité de vérifier que ce trafic est acceptable. Acceptable pour un firewall veut dire que tout ce qui y transite : e-mail, transfert de fichiers, login distant, ou toute interaction spécifique entre système, se conforme à la politique du site. Ces politiques diffèrent selon les sites.

Logiquement, un firewall est un séparateur, un limiteur, un analyseur. Ses implémentations varient selon les techniques du site. Il s'agit la plupart du temps d'un ensemble de composants matériels : Un routeur, Un ordinateur hôte, Une combinaison d'ordinateur, Des logiciels. [7] [9]

Toute la question est de savoir comment reconnaitre les paquets à accepter et à refuser. Il est possible de travailler de deux façons :

- Interdire tous les paquets sauf ceux d'une liste prédéterminée
- Accepter tous les paquets sauf ceux d'une liste prédéterminée

En règle générale le firewall utilise la première solution en interdisant tous les paquets, sauf ceux qu'il est possible d'authentifier par rapport à une liste des paquets que l'on souhaite laisser entrer. L'autre option est évidement beaucoup plus dangereuse puisque tous les ports sont ouverts sauf ceux qui ont été bloqués par la société. Une attaque ne se trouve pas bloquée tant qu'elle n'utilise pas les accès interdits.

Un firewall contient donc une table, qui indique les numéros de ports acceptés. Le tableau suivant présente les ports réservés de TCP les plus utilisés

N°port	Service	Commentaire
21	ftp	Protocole ftp
23	telnet	Protocole telnett
25	Smtp	Protocole smtp
53	domain	Serveur DNS
80	http	Service www
109	pop	Protocole POP

Tableau 5.01: *ports utilisés par TCP*

5.3 Avantages et inconvénients

5.3.1 Avantages

Les firewalls peuvent faire beaucoup de choses pour améliorer la sécurité d'un site. En fait, certains avantages dus à leur utilisation vont même bien au-delà de la sécurité.

5.3.1.1 Un firewall limite l'exposition

Un firewall sera parfois utilisé pour isoler une section du réseau d'un site d'une autre. On empêche de cette façon les problèmes qui touchent une section de se répandre dans tout le réseau. Une section est dans certains cas plus fiable, dans d'autre plus sensible, qu'une autre. [20] [21]

Quelle qu'en soit la raison, l'existence des firewalls limite les risques qu'un problème de sécurité fait encourir à tout le réseau.

5.3.1.2 Un firewall est au centre des décisions de sécurité

Pensez à un firewall comme un goulet d'étranglement. Tout le trafic entrant et sortant doit passer par cet étroit point de contrôle. Un firewall donne d'énormes possibilités parce qu'il permet de

concentrer les mesures de sécurité en ce point (l'endroit où le réseau est connecté à Internet). Cette manière de concentrer la sécurité est bien plus efficace que la diffusion des décisions et de technologies qui essaye de couvrir tous les domaines petit à petit. La plupart des sites estiment que la concentration des matériels et des logiciels les plus efficaces au niveau du firewall est moins chère et plus efficace que les autres mesures de sécurité. [20] [21]

5.3.1.3 Un firewall peut renforcer le règlement intérieur

Nombre de services que les gens désirent sur internet sont intrinsèquement dangereux. Le firewall joue le rôle d'un agent de circulation pour ces services. Il applique la politique de la sécurité du site, ne permettant qu'aux services approuvés de traverser, et uniquement dans le cadre des règles qui leur ont été affectées. Par exemple, la direction d'un site peut décider que certains services comme le NFS de Sun et le NIS sont beaucoup trop hasardeux pour être utilisés à travers du firewall. Peu importe que tel système ou tel utilisateur essaye de les employer. Le firewall confinera les services potentiellement dangereux à l'intérieur de la stricte enceinte du firewall. [21]

5.3.1.4 Un firewall peut facilement enregistrer l'activité internet

Comme tout le trafic passe par le firewall, il consiste un bon lieu de collecte d'informations sur l'utilisation des systèmes et du réseau, qu'elle soit bonne ou mauvaise. Le firewall, point d'accès unique, peut enregistrer ce qui se produit entre le réseau protégé et le réseau extérieur. [21]

5.3.2 Inconvénients

On a vu que les firewalls offrent une excellente protection contre les menaces réseau, mais ne constituent pas une solution complète de sécurité. Certains risques ne peuvent être contrôlés par eux. Il faut trouver d'autres moyens de protéger contre des menaces en incorporant une sécurité au niveau physique, au niveau des utilisateurs.

5.3.2.1 Un firewall ne peut protéger contre la connexion qui ne passe pas par lui

Un firewall peut efficacement contrôler le trafic qui passe par lui, il ne peut cependant rien faire si des connexions lui échappent. Et si par exemple, le système autorise des accès entrant derrière le firewall, il ne peut absolument rien contre un intrus passant par une de ces liaisons. Quelque fois, des utilisateurs experts ou des administrateurs système mettent en lace leurs propre entrées de service, à l'intérieur du réseau, qu'elle soit temporaire ou permanente, parce qu'ils ne peuvent supporter les restrictions que le firewall leur impose, à eux et à leurs systèmes. Le firewall n'y peut rien. Il s'agit là d'un problème d'encadrement, pas d'un problème technique. [20] [21]

5.3.2.2 Un firewall ne peut protéger contre des menaces complètement nouvelles

Un firewall est destiné à protéger contre des menaces connues. S'il est bien conçu, il peut également protéger contre des nouvelles menaces : par exemple, en interdisant tous les services sauf quelques uns considérés comme sûrs, il empêchera les gens de mettre en place des services nouveaux risqués. Cependant, aucun firewall ne peut automatiquement protéger défendre un site contre toutes une nouvelles attaques qui apparaissent. Les agresseurs découvrent régulièrement de nouvelles manières d'attaquer, en utilisant des services antérieurement sécurisés, ou en utilisant des méthodes qui n'ont jamais été essayées auparavant. [20] [21]

5.3.2.3 Sa mis en ouvre est un peu difficile

La mis en ouvre du firewall demande de la patience car elle est un peu difficile, de plus il parait difficile pour un utilisateur qui ne connait pas l'informatique de l'utiliser. [20] [21]

5.3.2.4 Le firewall ne peut pas protéger contre le virus

Les firewalls ne peuvent pas garder le PC et les virus de Macintosh hors d'un réseau. Bien que beaucoup des firewalls balayent tout le trafic entrant pour déterminer s' il est permis de passer à travers vers le réseau interne, le balayage est la plupart du temps pour des adresses de source et de destination et des nombres gauches, pas pour les détails des données. Même avec le logiciel de filtrage ou proxying sophistiqué de paquet, la protection de virus dans un mur à l'épreuve du feu n'est pas très pratique. Il y a simplement trop de types de virus et trop de manières qu'un virus peut se cacher dans des données. [20] [21]

Connaissant ses faiblesses pourquoi voudrait-on installer un ?

Firewall est un des outils les plus puissants en termes de sécurisation.

5.4 Conception d'un firewall

Cette partie nous explique, comment créer un firewall, comment créer le service pour les lancer, comment faire pour le maintenir, mais avant d'entamer ces paragraphes il est nécessaire de faire un petit rappel sur ce qu'on essaie de protéger, aux types d'attaques et aux types d'agresseurs.

5.4.1 Pourquoi mettre un firewall face à des feu Internet

Il n'est à peine possible d'entrer dans une librairie, a lu un magazine ou un journal, ou écoute une émission de nouvelles sans voir ou entendre quelque chose au sujet de l'Internet dans de l'apparence. On le devient si populaire qu'il n'exige plus des explications une fois mentionné en publications non techniques, et il obtient l'abondance mentionnée. Surtout pour une entreprise, des nouvelles documentations, des nouvelles publications, et aussi des nouveaux concurrents peuvent se trouver sur Internet. Des que vous connectez (l'entreprise), cela ouvre une autoroute à votre voisinage et invite bon nombre d'étranger à venir chez vous. Les deux vues sont vraies: L'Internet est un progrès technologique merveilleux qui permet d'accéder à l'information, et la capacité d'éditer l'information, des manières révolutionnaires. Mais c'est également un danger important qui fournit la capacité de polluer et détruire l'information des manières révolutionnaires. D'ou la nécessité d'un firewall Internet qui est une forme de protection permettant à un réseau de se relier à Internet tout en maintenant un degré de sécurité.

5.4.2 Rappel sur les attaques et les agresseurs

On a déjà vu sur le chapitre III, ce qu'on essaie de protéger et les types d'attaque mais il nécessaire de les rappeler.

5.4.2.1 Ce que vous essayez de protéger

Pour une entreprise et même pour un simple internaute, ce qu'on essaie de protéger :

- Les données
- Les réputations
- Les ressources

5.4.2.2 Les types d'attaques et les agresseurs

Il y a beaucoup de types d'attaques sur des systèmes, et beaucoup de manières de classer ces attaques par catégorie. On peut en citer quelques un comme

- Intrusion
- Refus de service
- Vol de l'information.

Il y a beaucoup de type d'agresseurs mais le plus souvent rencontrés sont :

- Les vandales
- Les espions

- Les maladresses
- Les plaisantais
- La stupidité ou plaisance

5.4.3 Quelques définitions utilisées sur le concept d'un firewall

Définition 5.02

Dans les paragraphes précédents on a présenté ce que c'est un firewall Internet, ce qu'il peut faire et ce qu'il ne peut pas faire, on a aussi fait un rappel concernant à ce qu'on essaie de protéger, aux types d'attaques, et aux types d'agresseurs. Dans le paragraphe suivant on va voir les principaux concepts des firewalls.

Firewall : Un composant ou un ensemble de composants qui limitent l'accès entre un réseau protégé et l'Internet, ou entre d'autres ensembles de réseaux. [21]

Hôte : un système informatique attaché à un réseau. [21]

Bastion hôte (Bastion host) : Un système informatique qui doit être fortement sécurisé parce qu'il est vulnérable à l'attaque, exposé à l'Internet et est un point principal de contact pour des utilisateurs des réseaux internes. [21]

Hôte à double réseau : Un système informatique d'usage universel qui a au moins deux interfaces réseau. [21]

Paquet : L'unité fondamentale de communication sur l'Internet. [21]

Filtrage de paquet : L'action qu'un dispositif prend pour commander sélectivement l'écoulement des données à et d'un réseau. Les filtres de paquet permettent ou bloquent des paquets, habituellement tout en les conduisant d'un réseau à l'autre (le plus souvent de l'Internet à un réseau interne, et vice versa). Pour accomplir le paquet filtrant, vous installez un ensemble de règles qui indiquent quels types de paquets (par exemple, ceux à ou d'un IP ADDRESS ou d'un port particulier) sont être permis et quels types doivent être bloqués. Le filtrage de paquet peut se produire dans un routeur, dans un pont, ou sur un centre serveur individuel. [21]

Réseau de périmètre : Un réseau s'est ajouté entre un réseau protégé et un réseau externe, afin de fournir une couche additionnelle de sécurité. Un réseau de périmètre s'appelle parfois un DMZ, qui représente la zone démilitarisée. [20] [21]

Serveur proxy : Un programme qui traite les serveurs externes au nom des clients internes. Les clients de procuration parlent aux serveurs de procuration, qui transmettent par relais des demandes approuvées de client dessus à de vrais serveurs, et le relais répond de nouveau aux clients. [20] [21]

5.4.3.1 Filtrage de paquet

Les systèmes de filtrage de paquet conduisent des paquets entre les centres serveurs internes et externes, mais ils le font sélectivement. Ils permettent ou bloquent certains types de paquets d'une manière dont reflète la propre politique de la sécurité d'un emplacement comme représenté sur la figure 5.02. Le type de routeur utilisé dans un firewall à filtrage de paquet est connu sous le nom routeur écran ou en anglais screening router.

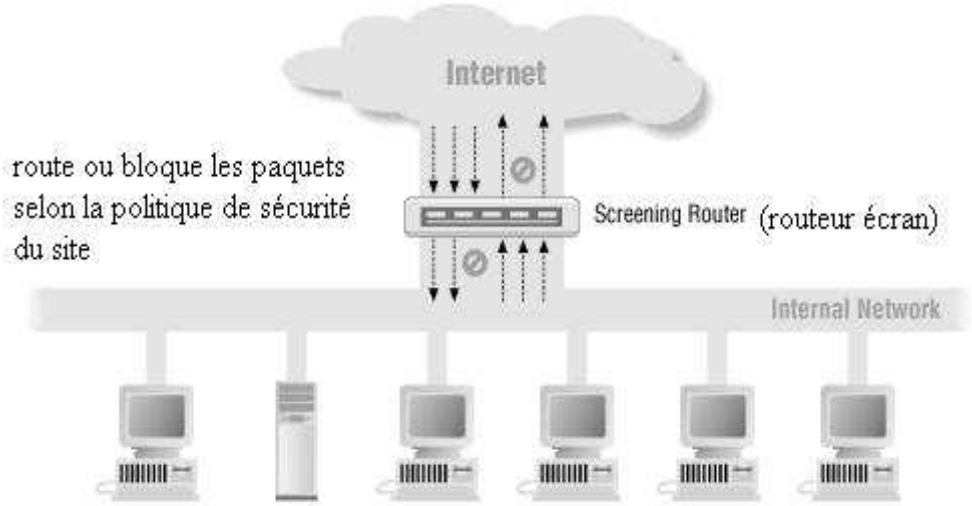

Figure 5.02 : *Utilisation d'un routeur écran pour faire le filtrage de paquet*

On a vu au premier chapitre que chaque paquet possède un ensemble d'en-têtes contenant une certaine information, l'information principale est :

- Adresse IP source
- Adresse IP destination
- Protocole (si le paquet est un paquet de TCP, d'UDP, ou d'ICMP)
- Port TCP ou UDP source
- Port de destination de TCP ou d'UDP
- Type de message d'ICMP

En outre, le routeur sait des informations au sujet du paquet qui ne sont pas reflétées dans les en-têtes de paquet, comme:

- L'interface où le paquet va arriver
- L'interface où le paquet va sortir

Le fait que les serveurs de certains services particuliers d'Internet résident à certain numéro de port permet au routeur de bloquer ou d'autoriser certains types de connexion simplement en indiquant le numéro de port approprié dans l'ensemble de règle de filtrage. [21]

Voici quelques exemples de façon à programmer un screening router ou routeur écran pour qu'il route sélectivement les paquets entrants ou sortants du site :

- Bloquez tous les raccordements entrants des systèmes en dehors du réseau interne, excepté les raccordements entrants de smtp (de sorte que vous puissiez recevoir l'email). [21]

- Bloquez tous les raccordements aux certains systèmes que vous méfiez. [21]
- Permettez l'email et les services de ftp, mais bloquez les services dangereux comme TFTP, le système de fenêtre de X Windows, le RPC, et les services de " r " (rlogin, rsh, RCP, etc.). [21]

Pour comprendre comment fonctionne le filtrage de paquet, observons la différence entre le routeur ordinaire et le routeur écran

Un routeur ordinaire regarde simplement l'adresse de destination de chaque paquet et sélectionne la meilleure manière qu'elle sait pour envoyer ce paquet vers cette destination. Cette décision est basée seulement sur sa destination. Il y a deux possibilités: le routeur sait comment atteindre et envoyer le paquet vers sa destination; ou le routeur ne sait pas envoyer le paquet vers sa destination, et elle renvoie le paquet, par l'intermédiaire d'un ICMP de type destination inaccessible vers la source. [21]

Un screening router ou routeur écran, d' autre part, regarde des paquets plus étroitement. En plus de déterminer s'il peut conduire un paquet vers sa destination, mais il détermine également s'il devrait ou il ne devrait pas selon la politique du site.

Bien qu'il soit possible que seulement un routeur écran se repose entre un réseau interne et l'Internet, comme représenté sur la figure 5.02, ceci place une énorme responsabilité sur le

routeur écran. Non seulement, il doit exécuter tous les routages et les prises de décision selon les politiques du site, mais c'est le seul système protecteur; si sa sécurité échoue (ou s'émiette sous l'attaque), le réseau interne est exposé. En outre, un routeur écran ne peut pas modifier des services. Il peut permettre ou nier un service, mais il ne peut pas protéger différentes opérations dans un service. Si un service souhaitable a des opérations peu sûres, ou si le service est normalement équipé de serveur peu sûr, le filtrage de paquet seul ne peut pas le protéger.

5.4.3.2 Proxy service

La traduction de proxy service en français c'est service de procuration mais gardons le terme proxy service à tout ce qui suit.

Un proxy est une application qui sert d'intermédiaire entre un client et un serveur. Le client envoie sa requête au proxy, et celui-ci la réémet en direction du serveur. De même, la réponse du serveur est reçue par le proxy qui la retransmet au client. Un proxy peut être configuré pour filtrer les requêtes. Pour cette raison, des proxy sont parfois connues comme passages d'application-niveau. Des logiciels proxy peuvent posséder de la manière cache, RAM et disque, ce qui améliore les performances d'accès des postes du réseau intérieur. [20] [21]

Les services proxy se reposent, plus ou moins d'une manière transparente, entre un utilisateur sur l'intérieur c'est à dire sur le réseau interne et un service sur l'extérieur c'est à dire sur l'Internet. Au lieu de parler entre eux directement, chacun parle à un proxy. Les proxy manipulent toute la communication entre les utilisateurs et les services d'Internet dans les coulisses. Le transparent est l'avantage principal des services proxy. À l'utilisateur, un serveur proxy présente l'illusion que l'utilisateur traite directement le vrai serveur. Au vrai serveur, le serveur proxy présente l'illusion que le vrai serveur a affaire directement avec un utilisateur sur le centre serveur de proxy. [20] [21]

Comment les services proxy fonctionnent-ils? Regardons le cas le plus simple, où nous ajoutons des services de proxy à un dual-homed host. Comme indique la figure 5.03, un service proxy exige deux composants: un proxy serveur et un proxy client. Dans cette situation, le proxy serveur fonctionne sur le dual-homed host. Un proxy client est une version spéciale d'un programme normal de client (un client comme telnet ou ftp) ; en outre, si on enseigne des utilisateurs des procédures spéciales à suivre, des programmes normaux de client peuvent souvent être employés comme clients de proxy. Le proxy serveur évalue des demandes du client proxy, et décide ce qui est à approuver et ce qui est à nier. Si une demande est approuvée, le proxy serveur entre en contact avec le vrai serveur au nom du client, et le

transmettre par relais des demandes du client au vrai serveur, et des réponses du vrai serveur au client.

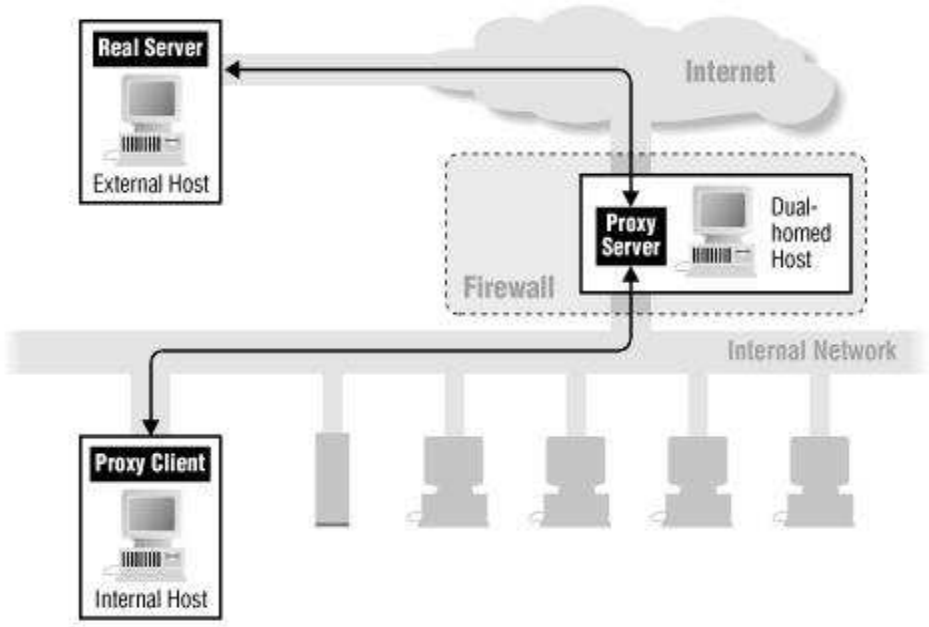

Figure 5.03 : *utilisation des services de procuration avec un dual-homed host*

Le proxy serveur n'expédie pas toujours les demandes d'utilisateurs aux vrais services d'Internet. Le proxy serveur peut commander quels sont les utilisateurs en travail, parce qu'il peut le faire à des décisions au sujet des demandes des processus. Selon la politique de la sécurité de votre emplacement, des demandes pourraient être permises ou refusées. Par exemple, la procuration de ftp pourrait refuser a laissé des utilisateurs exporter des dossiers, ou elle pourrait permettre à des utilisateurs d'importer des dossiers seulement de certains emplacements. Des services plus sophistiqués de procuration pourraient permettre différentes possibilités à différents centres serveurs, plutôt que d'imposer les mêmes restrictions à tous les centres serveurs.

5.4.3.3 Utilisation d'une combinaison de technique et de technologie

La bonne solution pour construire un firewall est rarement un technique simple; c'est habituellement une combinaison soigneusement des plusieurs techniques pour résoudre différents problèmes. « Quels problèmes vous devez résoudre » dépendent de « quels services voulez vous pour fournir vos utilisateurs » et « quels niveaux de risque vous êtes disposé à accepter ». « Quelles techniques vous employez pour résoudre ces problèmes » dépendent de « combien d'heure, d'argent, et d'expertise avez vous disponible ». Quelques protocoles (par exemple, telnet et smtp) peuvent plus efficacement être manipulés avec le filtrage de paquet.

D'autres (par exemple, ftp, Archie, Gopher, et WWW), plus efficacement, sont manipulés avec des proxys. La plupart de firewall emploie une combinaison de proxying et de filtrage de paquet. [20] [21]

5.5 Architecture d'un firewall

Il existe plusieurs façons d'assembler les composants d'un firewall. Toutes les architectures dépendent de la politique de sécurité adoptée et le niveau de sécurité qu'on veut obtenir.

5.5.1 Architecture d'hôte à double réseau

Une architecture d'hôte à double réseau est établie autour d'un ordinateur à double réseau, qui a au moins deux interfaces. Un tel hôte pourrait agir comme un routeur entre les réseaux auxquels sont attachées les interfaces; il est capable d'acheminer les paquets d'IP d'un réseau à l'autre. Cependant, il faut désactiver cette fonction de routage pour implémenter une architecture de type hôte à double réseau. Ainsi, des paquets d'IP d'un réseau (comme l'Internet) ne sont pas directement conduits à l'autre réseau (par exemple le réseau interne protégé). Les systèmes à l'intérieur du firewall peuvent communiquer avec l'hôte à double réseau, ainsi que les systèmes en dehors du firewall c'est à dire ce qui est situé sur l'internet, mais ces systèmes ne peuvent pas communiquer directement avec l'un à l'autre. Le trafic d'IP entre eux est complètement bloqué. La figure suivante permet de représenter l'architecture de l'hôte à double réseau. [20] [21]

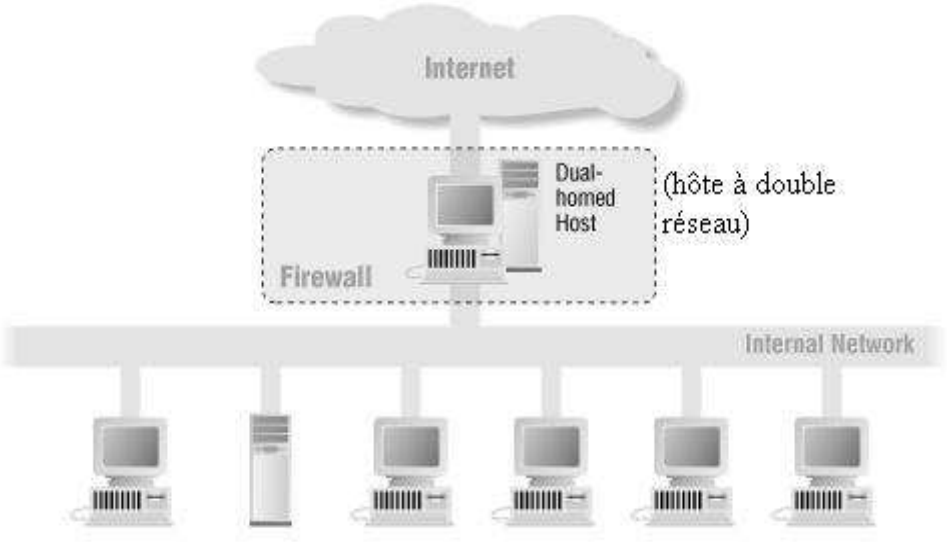

Figure 5.04 : *Architecture d'hôte à double réseau*

Les hôtes à double réseau peuvent fournir un niveau très élevé de contrôle. Si on ne permet à aucun paquet d'aller directement entre les réseaux externes et internes, on est sûr que tout

paquet du réseau interne qui provient d'une source extérieure prouve l'existence d'erreur. Dans certains cas, l'hôte à double réseau permettra de rejeter cette connexion qui prétend être pour un service particulier, mais qui ne contient pas réellement le bon genre de données. Cependant, il faut un travail considérable pour bénéficier des avantages potentiels des hôtes à double réseau.

les hôtes à double réseau ne peuvent fournir des services que par mandatement (proxying), ou en laissant les utilisateurs se connecter directement sur l'hôte. Le mandatement est moins problématique mais peut ne pas être disponible pour tous les services qui vous intéressent. L'architecture de sous-réseau à écran qu'on va décrire au dessous offre quelques options supplémentaires pour fournir des services nouveau.

5.5.2 Architecture d'hôte à écran

Considérant qu'une architecture d'hôte à double écran fournit des services depuis un hôte qui est attaché aux réseaux multiples, mais dont le routage est désactivé, une architecture d'hôte à écran fournit des services depuis un hôte qui est attaché seulement au réseau interne, à l'aide d'un routeur séparé. Dans cette architecture, la sécurité primaire est fournie par le filtrage de paquet. (Par exemple, le filtrage de paquet est ce qui empêche les gens de contourner les serveurs mandataires pour établir des connexions directes). [20] [21]

La figure 4.06 montre une version simplifiée de l'architecture d'hôte à écran

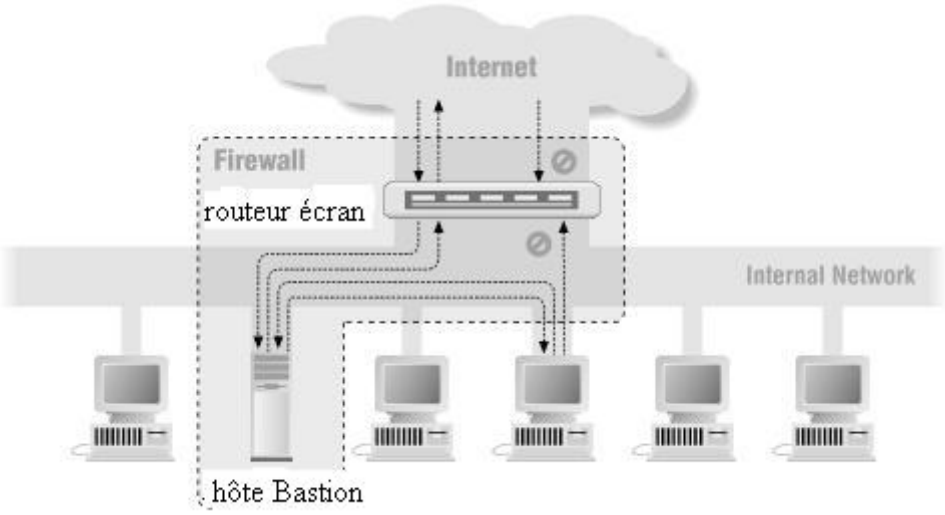

Figure 5.05 : *Architecture d'hôte à écran*

Le Bastion se repose sur le réseau interne. Le filtrage de paquets sur le routeur écran est mis en place de telle façon que le bastion est le seul système sur le réseau interne auquel peuvent accéder les hôtes sur l'internet. Même dans ce cas, seules certaines connexions sont autorisées.

N'importe quel système externe essayant d'accéder aux systèmes ou aux services internes devra se relier à ce cet hôte. Le bastion doit ainsi maintenir un niveau élevé de degré de sécurité hôte. Le filtrage de paquet permet également au bastion d'ouvrir des connexions acceptables vers le monde extérieur (la signification du terme acceptable est déterminée par la politique du site). La configuration de filtrage de paquet d'un routeur écran peut faire un de ce qui suit:

- Permettre à d'autres hôtes internes d'ouvrir des connexions vers les hôtes sur Internet pour certains services.
- Interdire toutes les connexions depuis des hôtes internes.

Il est possible de mélanger et assortir ces approches pour différents services; certains peuvent être permis directement par le filtrage de paquets, alors que d'autres ne peuvent être autorisés que par mandatement. Tout dépend de la politique particulière qu'un site essaye de faire respecter.

Cette architecture permet à des paquets de se déplacer de l'Internet aux réseaux internes, elle peut sembler être plus risqué qu'une architecture d'hôte à double réseau, qui est conçue de sorte qu'aucun paquet externe ne puisse atteindre le réseau interne. Dans la pratique, cependant, l'architecture d'hôte à double réseau est également encline aux échecs qui laissent des paquets réellement croiser du réseau externe au réseau interne. En outre, il est plus facile de défendre un routeur, qui fournit un nombre limité de service, qu'un ordinateur. L'architecture d'hôte à écran fournit, dans la plupart des cas, une meilleure sécurité et une meilleure rentabilité que l'architecture d'hôte à double réseau. Cependant il existe certains inconvénients à l'architecture d'hôte à écran. Le principal est que, si un attaquant parvient à s'introduire au bastion, plus rien ne s'interpose entre lui et le reste du réseau. Le routeur présente également un point unique de défense s'il est mis en échec, l'intégralité du réseau devient accessible à l'agresseur. [21]

5.5.3 Architecture de sous réseau à écran

L'architecture de sous réseau à écran ajoute une couche supplémentaire à l'architecture d'hôte à écran en ajoutant un réseau périphérique qui isole encore plus le réseau interne de l'Internet.

Le type d'architecture le plus simple comprend deux routeurs écrans, chacun connecté au réseau périphérique. L'un des deux est situé entre le réseau périphérique et le réseau interne, et l'autre entre le réseau périphérique et le réseau externe. Pour s'introduire dans le réseau interne avec ce type d'architecture, un agresseur devrait passer par les deux routeurs. Même arrivait au bastion,

il devrait encore passer à travers le routeur interne, il n'y a plus d'unique point vulnérable qui mettrait en danger le réseau intérieur. [20] [21]

Quelques emplacements vont autant que créer une série de couches périphériques entre le réseau extérieur et leur interne. Les services moins fiables et les plus vulnérables sont placés sur les réseaux périphériques extérieurs, loin du réseau interne. L'idée est qu'un attaquant qui pénètre par effraction dans une machine d'un réseau périphérique externe trouvera plus difficile d'attaquer successivement toutes les machines internes en raison de couches additionnelles de sécurité entre le périphérique extérieur et le réseau interne. Mais ceci n'est vrai que si les couches intérieures ont une réelle raison d'être; si les systèmes de filtrage entre chaque couche permet les mêmes choses entre toutes les couches, les couches additionnelles ne fournissent aucune amélioration de la sécurité. Avec un réseau périphérique, si quelqu'un pénètre dans le bastion du réseau périphérique, il ne peut espionner que le contenu de ce réseau.

Voici une figure permettant de représenter une architecture de sous écran à écran

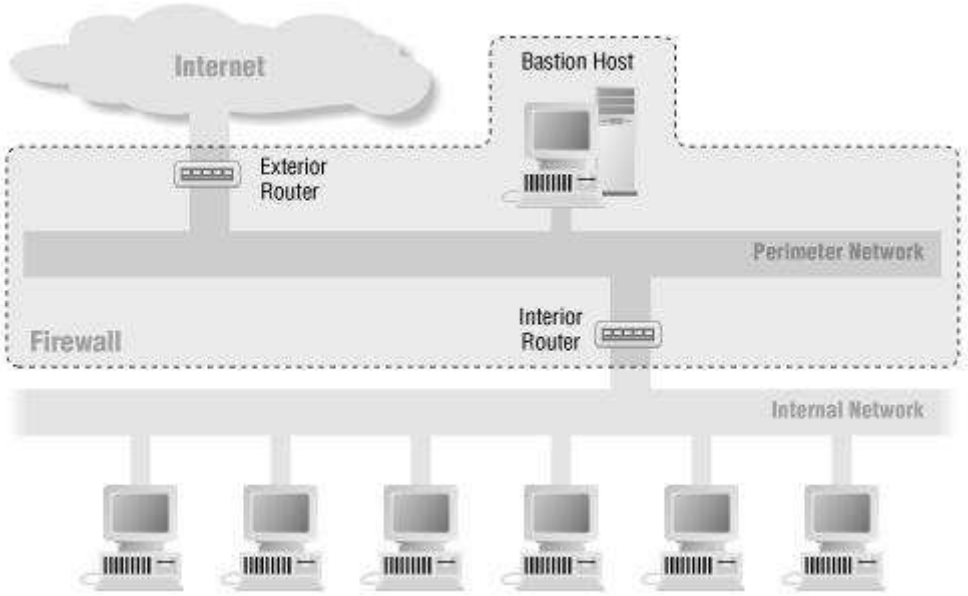

Figure 5.06 : *Architecture de sous réseau écran*

5.5.3.1 Réseau de périphérique

Le réseau de périphérique est une autre couche de sécurité. C'est un réseau additionnel entre le réseau externe et le réseau interne protégé. Si un attaquant parvient à casser le firewall, le réseau de périmètre (périphérique) offre une couche additionnelle de protection entre cet attaquant et les systèmes internes. [21]

Voici un exemple, pourquoi un réseau de périphérique peut être utile. Dans beaucoup d'installations de réseau, il est possible que n'importe quelle machine sur un réseau donné voie le trafic pour chaque machine sur ce réseau. Cela peut ; pour la plupart de réseau comme Ethernet, FDDI, Token Ring, connaitre les différents mots de passe sur les machines. Même si des mots de passe ne sont pas compromis, les agresseurs peuvent encore jeter un coup d'œil sur les teneurs des dossiers sensibles que les gens peuvent accéder, email intéressant ils peuvent lire les emails intéressant, et ainsi de suite.

5.5.3.2 Fonctionnement d'un Bastion

Avec l'architecture examinée de sous réseau à écran, on attache un bastion au périphérique; cet hôte est le principal point de contact pour les connexions depuis le monde extérieur; par exemple:

- Pour les sessions e-mail entrantes (smtp) pour fournir le courrier électronique
- Pour les connexions FTP entrantes sur le serveur FTP anonyme
- Pour les requêtes DNS entrantes concernant le site

Pour les services sortants, c'est-à-dire depuis le client interne vers l'internet, sont selon l'une des méthodes suivantes

- Régler le filtrage de paquet sur les routeurs extérieurs et intérieurs afin de permettre à des clients internes d'accéder directement aux serveurs externes.
- Au cas où le firewall utilise un logiciel mandataires, configurer les serveurs mandataires tournant sur l'hôte bastion, pour permettre aux clients internes d'accéder indirectement aux serveurs externes. Il faut aussi régler le filtrage de paquets pour permettre aux clients internes de parler aux serveurs mandataires du bastion et vice versa, mais interdire les communications directes entre les clients internes et le monde extérieur.

Dans tout les cas, le filtrage de paquet permet au bastion de se connecter aux hôtes de l'internet et d'accepter les connexions provenant de ces derniers, les choix de ces hôtes et des services utilisés est dicté par la politique de sécurité du site. Le bastion se comporte essentiellement en serveur mandataire pour des services variés, que ce soit par l'intermédiaire d'un logiciel de serveur mandataire spécialisé pour des protocoles particuliers (comme http ou FTP), ou en faisant tourner des serveurs standard pour des protocoles à mandatement intégré (comme SMTP). [21]

5.5.3.3 Routeur intérieur

Le routeur intérieur protège le réseau interne contre l'Internet et du réseau de périphérique.

Il fait la majeure partie du filtrage de paquet du firewall. Il permet des services choisis de sortir de l'interne vers l'Internet. Ces services sont ceux qu'un site peut supporter et fournir en toute sécurité en utilisant un filtrage de paquet au lieu de mandatement. On devra considérer les propres besoins, possibilités, et contraintes car il n'y a pas une seule réponse pour tous les emplacements. Les services qu'on permet peuvent inclure le Telnet, le ftp, le WAIS, l'Archie, le Gopher, et autres sortants, selon les besoins et les préoccupations. Les services que le routeur intérieur autorise entre le bastion et le réseau interne ne sont pas nécessairement les mêmes que le routeur intérieur autorise entre l'internet et le réseau interne. Le but à cela ce qu'il faut limiter le nombre de machines qui peuvent être attaqués depuis le bastion en cas d'intrusion réussie sur celui-ci. [21]

On doit limiter les services permis entre le bastion et le réseau interne, on autorise ceux qui sont réellement nécessaires, comme le smtp (ainsi le bastion peut expédier l'email entrant), le DNS (ainsi le bastion peut répondre à des questions des machines internes, ou demander, selon la configuration), et ainsi de suite. On doit encore plus restreindre ces services, si possible, en ne les autorisant que vers ou depuis des hôtes spécifiques, par exemple, le smtp peut être limité seulement aux connexions entre le bastion et le serveur du mail interne. Prêtez une attention particulière au degré de sécurité des hôtes et services qui peuvent être entrés en contact par le bastion, car ils seront les cibles privilégiée d'un agresseur, le seul possible en fait s'il réussit à pénétrer dans le bastion. [21]

5.5.3.4 Routeur extérieur

En théorie, le routeur extérieur protège à la fois le réseau de périphérique et le réseau interne contre l'Internet. Dans la pratique, les routeurs extérieurs tendent à laisser passer presque touts les services sortants, et ne font que très peu de filtrage de paquets. Les règles de filtrage qui protègent les machines internes devraient être à peu près le même sur les deux routeurs externes et internes; s'il y a une erreur dans les règles qui permet l'accès à un attaquant, l'erreur sera probablement présente sur les deux routeurs. Fréquemment, le routeur extérieur est relié par un groupe externe (par exemple, le fournisseur Internet), et son accès est donc limité. Le groupe externe qui maintient le routeur sera probablement disposé à mettre quelques règles de filtrage de paquet, mais ne voudra pas maintenir une règle compliquée et fréquemment changée. On ne peut pas également leur faire confiance autant qu'on fait confiance au propre routeur. Si le routeur se casse et ils installent un neuf, vont-ils se rappeler de réinstaller les filtres?. Les seules

règles de filtrage de paquets qui soient vraiment spécifiques au routeur sont celles qui protègent les machines sur le réseau de périphérique, c'est-à-dire le bastion et le réseau interne. Elles bloquent le trafic peu sûr entre les hôtes internes et l'Internet. Ainsi, qu'est ce que le routeur extérieur doit-il réellement faire? Un des tâches de sécurité que le routeur extérieur peut utilement accomplir et une tâche qui habituellement ne peut pas facilement être faite n'importe où est le blocage de tous les paquets entrants de l'Internet qui ont forgé des adresses de source. [21]

Il existe plusieurs variations d'architecture du Firewall, par exemple :

- L'utilisation de plusieurs bastions : il est bien d'utiliser plusieurs bastions pour raisons d'exécution, redondance, et la nécessité de séparer les données ou serveurs. On peut avoir une poignée de bastion pour les services important de l'utilisateur pendant que l'autre manipule les services venant de l'internet.
- Le fusionnement du routeur extérieur et intérieur : on peut fusionner les routeurs intérieurs et extérieurs dans un seul routeur, mais seulement si on a un routeur suffisamment capable et flexible. En général, on a besoin d'un routeur qui permet d'indiquer les filtres d'arrivée et sortant sur chaque interface.
- L'utilisation du bastion et de routeur extérieur
- L'utilisation de plusieurs routeurs extérieurs

Néanmoins il est déconseillé d'utiliser :

- Des multiples routeurs intérieurs
- De fusionner un routeur intérieur et un bastion

5.6 Réalisation du Firewall

5.6.1 Rappels

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne) ;
- une interface pour le réseau externe.

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

- La machine soit suffisamment puissante pour traiter le trafic ;
- Le système soit sécurisé ;
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

Le firewall est constitué d'un :

- Routeur filtrant : est un routeur qui transfère les paquets IP entre Internet et le LAN. Il peut être configuré pour ne laisser passer que certains paquets.
- Proxy : un proxy est une application qui sert d'intermédiaire entre un client et un serveur. Le client envoie sa requête au proxy, et celui –ci la réémet en direction du serveur. De même, la réponse du serveur est reçue par le proxy qui la retransmet au client.
- Rempart : un rempart ou Bastion Host est un ordinateur accessible de l'extérieur, côté Internet, et qui est donc vulnérables aux attaques.

Il existe plusieurs architectures du firewall

- L'architecture « Dual-Homed » (hôte à double réseau ou machine multi-domicilée) : le rempart relie les deux réseaux mais il ne route pas les paquets. Il abrite les proxys et les services réseaux.
- L'architecture « screening router », construite autour d'un routeur filtrant.
- L'architecture « screened subnet », constituée d'un ou plusieurs remparts reliés à deux routeurs filtrants, l'un protège le rempart de l'extérieur et l'autre sépare le réseau interne des remparts.

SOCKS : l'architecture SOCKS comprend un serveur SOCKS et des clients SOCKS sous forme de bibliothèque, ces bibliothèques remplacent les bibliothèques ordinaires d'accès au réseau. [20]

IP Masquerading : traduction d'adresse, permettant de voir un ensemble d'ordinateurs comme une seule machine.

Les principaux outils de configurations de firewall sont :

- Routeur filtrant :

Sous linux on peut configurer un routeur filtrant avec les paquetages :

  - Ipfwadm
  - Ipchains
  - Netfilter/iptables

- Ordinateur multi-domicilié avec proxy

  On installe des applications proxys en utilisant le squid

5.6.2 Réalisation du firewall avec Netfilter/Iptables

Pendant cette étude, on va prendre :

Une machine, nommée monentreprise, qui est se trouve dans un réseau privé nommé entreprise.mg et possédant une adresse IP 192.168.10.2

Une machine, nommée Phoenix, qui relie le réseau privé avec l'internet donc il possède deux cartes réseaux, l'interface pour liée Phoenix avec le réseau privé est eth0 avec une adresse IP 192.168.10.1. Celui qui relie Phoenix avec l'internet est l'interface eth1 avec une adresse 10.0.0.1

Une machine, nommée pirate, qui se trouve sur Internet avec une adresse 10.0.0.4, son rôle est donc de pirater la machine monentreprise. La figure suivante permet d'illustrer cette architecture.

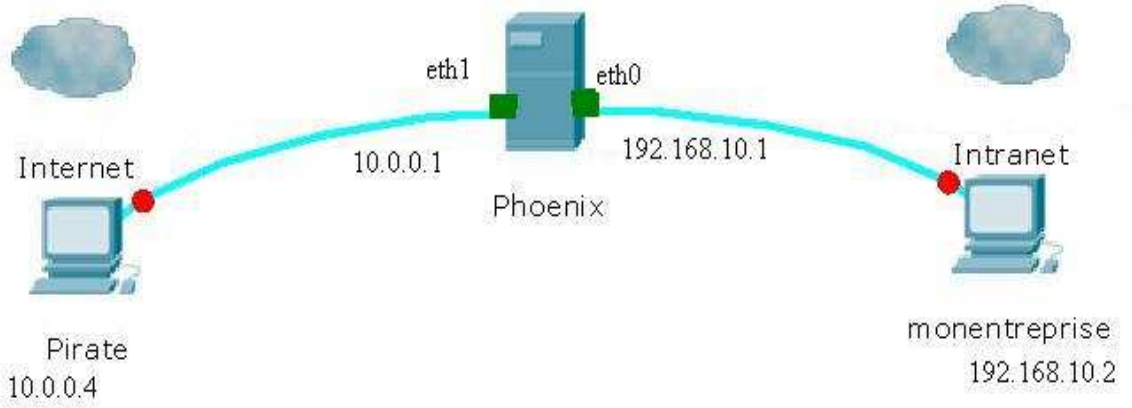

Figure 5.07 : *Architecture des machines*

Voici quelques outils d'analyse et de détection :

Nmap, Tcpdump, Ethereal, Netstat, Lsof, Fuser, Ping, Traceroute. A l'aide de ces outils un pirate qui se trouve sur l'internet peut détecter une machine de l'entreprise qui est connecté sur internet.

5.6.2.1 Vue générale du Netfilter

Netfilter peut intervenir en 5 endroits du système de gestion de la pile IP. Pour chacune de ces étapes (que l'on appelle des "hook", pour "crochet" en français), Netfilter peut :

- Imposer au kernel de supprimer le paquet ("drop" en anglais). Auquel cas, il est jeté aux oubliettes, et c'est comme si le paquet n'avait jamais existé.
- Indiquer au kernel que le paquet est accepté. Dans ce cas là, le kernel peut continuer à travailler dessus.
- Modifier le paquet, puis le rendre au kernel.

un "hook" est l'équivalent, dans la couche IP, d'une interruption (matérielle ou logicielle) : Lorsque qu'un événement arrive, le système d'exploitation arrête les tâches en cours, et exécute un morceau de code particulier. Une fois que ce code est fini, le système continue son travail comme si rien ne s'était passé. La figure 4.08 permet d'illustrer ce hook ou point d'accrochage

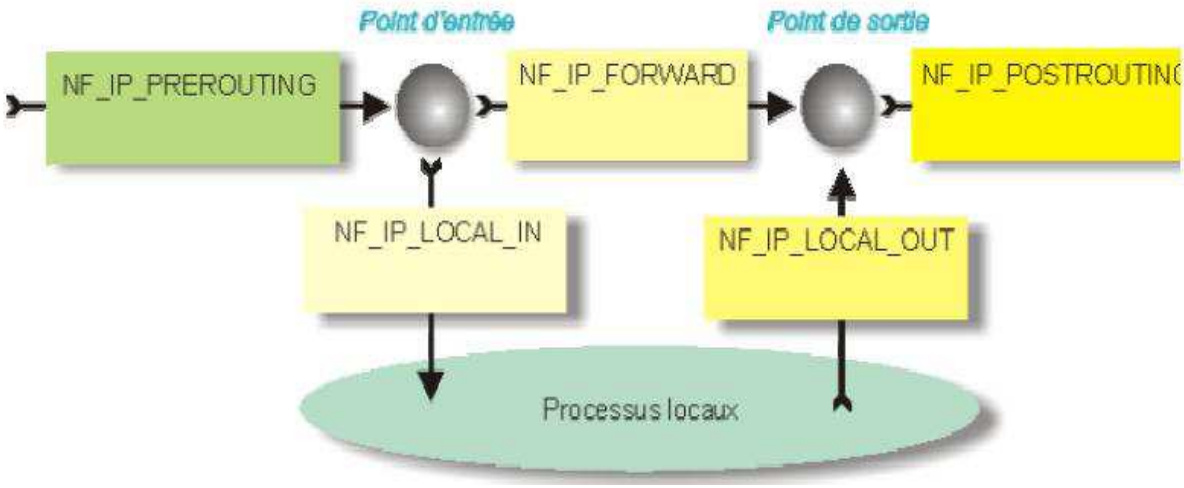

Figure 5.08 : *point d'accrochage*

A travers de ces cinq points d'insertion, NetFilter va être capable :

- D'effectuer des filtrages de paquets, principalement pour assurer des fonctions de Firewall. On pourra par exemple interdire à tous les paquets venant de l'internet et s'adressant au port 80 (http) de passer. Notre serveur apache est un serveur Intranet et ne doit pas être accessible depuis l'extérieur

- D’effectuer des opérations de NAT. Ces fonctions sont particulièrement utiles lorsque l’on veut faire communiquer tout ou partie d’un réseau privé monté avec des adresses IP privées avec l’Internet
- D’effectuer des opérations de marquage des paquets, pour leur appliquer un traitement spécial. Ces fonctionnalités sont particulièrement intéressantes sur une passerelle de réseau d’entreprise, un peu moins pour le réseau privé

Comment Netfilter sait le faire ? Netfilter dispose d’une commande à tout faire : Ipatbles. Cette commande va permettre entre autres, d’écrire des chaines dans des tables.

Une chaîne est un ensemble de règles (du type "si quelque chose alors je fais ceci") concernant les paquets IP : leur origine, leur destination, leur taille, etc. En fonction des différentes règles de la chaîne, Netfilter pourra décider quoi fait du paquet IP : Le laisser passer, le supprimer ou le modifier.

Le tableau suivant permet de décrire les cinq hook et leurs chaines.

hook	chaine	description
NF_IP_PRE_ROUTING	PREROUTING	A ce stade, le paquet est "brut de forme", c’est à dire qu’il n’a subit aucune modification par rapport à ce que l’interface réseau a reçu.
NF_IP_LOCAL_IN	INPUT	à ce stade, le paquet est prêt à être envoyé aux couches applicatives, c’est à dire aux serveurs et aux clients qui tournent sur la machine.
NF_IP_FORWARD	FORWARD	Ce "hook" voit passer des paquets IP qui vont transiter d’une interface réseau à une autre, sans passer par la couche applicative, permettre à Linux de se transformer en passerelle
NF_IP_LOCAL_OUT	OUPUT	Ce "hook" est l’équivalent du NF_IP_LOCAL_IN", sauf qu’il est exécuté après que les couches applicatives aient traités, ou générés, un paquet IP. Tout comme "NF_IP_LOCAL_IN",
NF_IP_POSTROUTING	POSTROUTING	C’est l’équivalent du "NF_IP_PRE_ROUTING" pour les paquets IP sortants de la couche IP. A ce stade, les

		paquets sont prêts à être envoyés sur l'interface réseau.

Tableau5.02 : *résumant le Hook et la chaine*

5.6.2.1.1 Table

Une table permet de définir un comportement précis de Netfilter. Une table est en fait un ensemble de Chaînes, elles-mêmes composées de règles. Donc, c'est la table qui va nous permettre de manipuler Netfilter, afin de lui faire faire des choses intéressantes. [22]

Il existe trois tables :

- Filter
- NAT
- MANGLE

a) La table Filter

Cette table va contenir toutes les règles qui permettront de filtrer les paquets. Cette table contient trois chaines :

- INPUT : cette chaine contrôle les paquets à destination des applications. [22]
- OUTPUT : elle analyse les paquets qui sortent des applications. [22]
- FORWARD : Elle filtre les paquets qui passent d'une interface réseau à l'autre. Il faut noter qu'au passage les paquets de ce type ne passent jamais par les chaînes INPUT et OUTPUT. [22]

Illustrons ces chaines à l'aide d'une figure

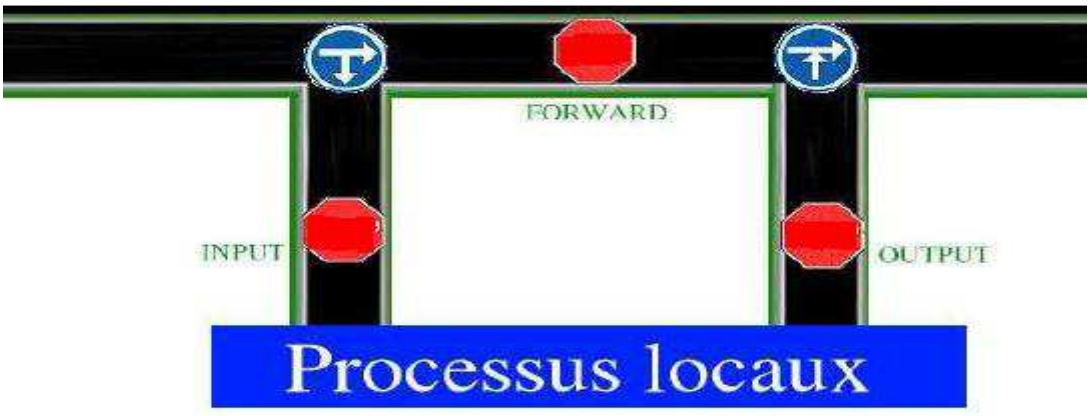

Figure 5.09 : *chaines de la table filter*

b) La table NAT

Cette table permet d'effectuer toutes les translations d'adresses nécessaires. [22]

Elle contient trois chaines :

- PREROUTING : Les paquets vont être modifiés à l'entrée de la pile réseaux, et ce, qu'ils soient à destination des processus locaux où d'une autre interface.
- OUTPUT : Les paquets sortant des processus locaux sont modifiés.
- POSTROUTING : les paquets qui sont près à être envoyés aux interfaces réseaux sont modifiés.

La figure suivante permet d'illustrer ces chaines

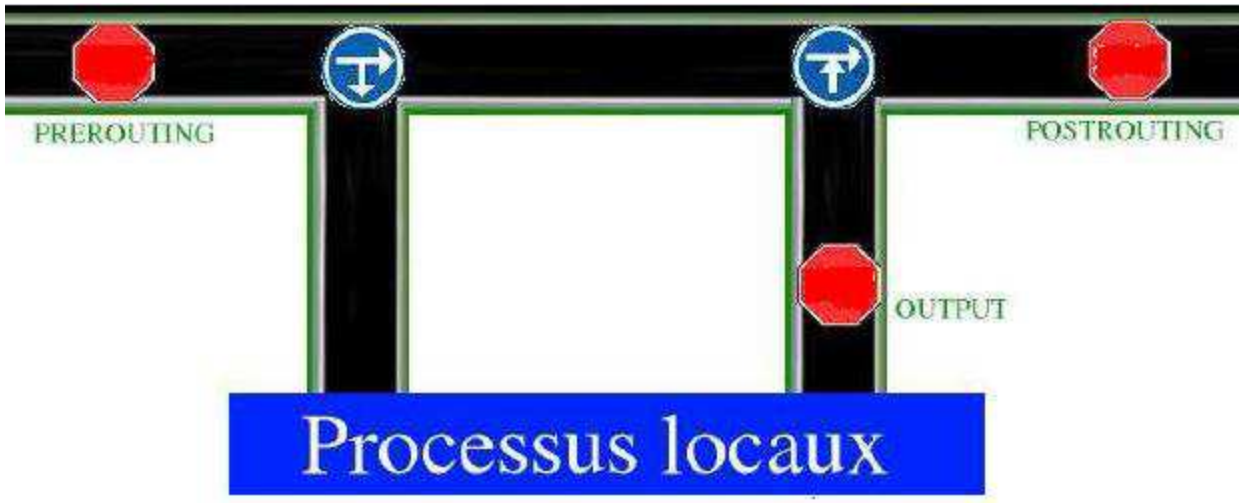

Figure 5.10 : *chaines de la table NAT*

c) La table Mangle

Il s'agit de marquer les paquets en entrée de la couche réseau, afin que d'autres programmes de l'espace kernel ("kernel space") puissent en faire quelque chose. L'idée de cette technique est par exemple de fournir à Linux la possibilité d'avoir un contrôle sur les débits des flux de données entrants et sortants de la machine, afin de rendre certains flux plus prioritaires que d'autres. [22]

Elle utilise les chaines du Netfilter :

- PREROUTING : Les paquets vont être marqués en entrée de la couche réseau, en fonction de certains critères, de type de service (grâce aux numéros de ports source et/ou de destination), d'adresses IP de source et/ou de destination, de taille des paquets, etc. Ces informations seront utilisées par un programme fonctionnant dans l'espace kernel.
- INPUT : Les paquets sont marqués juste avant d'être envoyés aux processus locaux.
- FORWARD : Les paquets passant d'une interface réseau à l'autre sont marqués.
- OUTPUT : Là, ce sont les paquets générés par les applications locales (un client web par exemple) qui vont être marqués, tout comme les paquets entrant dans la couche réseau.

- POSTROUTING : Les paquets prêts à être envoyés sur le réseau sont marqués. L'utilisation de cette chaîne dans la table Mangle n'est cependant pas très évidente.

La figure suivante permet de visualiser ces chaines

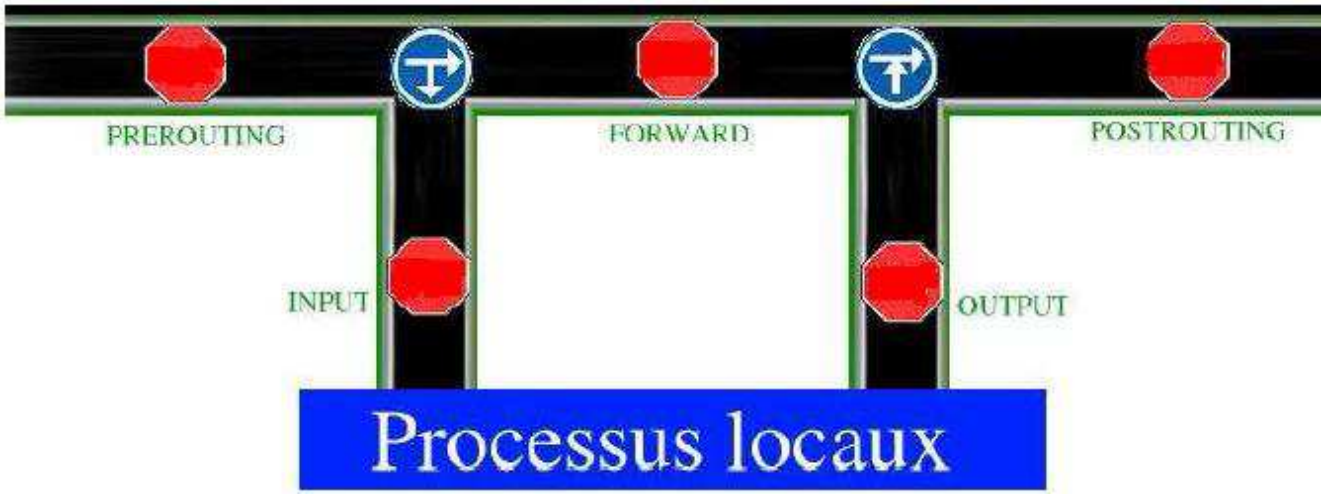

Figure 5.11 : *chaines de la table mangle*

- Les chaines utilisateurs

Ces sont des ensembles des règles que Netfilter parcourra afin de décider quoi faire des paquets. [22]

- Règles et cible

Les règles, comme leur nom l'indique, sont une série de critères auquel doivent ou non répondre les paquets. En fait. Si le paquet réseau ressemble à l'un ou l'autre des critères, alors la règle est appliquée. Les différentes règles d'une chaînes sont appliquées les unes à la suite des autres. [22]
Les critères peuvent être multiples : Interface source ou destination, Adresse IP source ou de destination, Port source ou de destination. Type de trame, Nombre de paquets Paquet marqué par la table Mangle, Etc.
Il peut y avoir autant de règles que l'on veut dans une chaîne, mais il est intéressant de limiter au maximum leur nombre, afin d'avoir une vue claire et précise de notre système de filtrage.
Enfin, à chaque règle est associée une action (ou "CIBLE" dans la nomenclature de Netfilter) à effectuer si la règle doit s'appliquer. C'est là que Netfilter agit, qu'il fait quelque chose avec le paquet réseau. Les principales actions sont :

- DROP : Le paquet est détruit purement et simplement.
- ACCEPT : Le paquet a une "bonne tête", il est donc autorisé à continuer à passer. Mais une autre règle située après la règle qui a accepté ce paquet peut très bien finalement décider de le supprimer.

- LOG / ULOG : Le paquet est autorisé à continuer de passer, mais ses caractéristiques sont notées au passage. En général, c'est qu'on estime que le paquet est "louche", et que l'on veut en prendre note. Mais plus souvent encore, on décidera de le supprimer.
- MASQUERADE : Le paquet va être modifié, afin de dissimuler (de masquer en fait) certaines informations concernant son origine. Cette technique sera utilisée un peu plus loin.
- MARK : le paquet est marqué en y attachant une information. Ceci est principalement utilisé avec les tables "Mangle"

5.6.2.1.2 *Iptables*

Iptables est une commande que seul le root peut lancer. Son but est de dialoguer avec Netfilter, afin de contrôler les règles des chaînes, dans le but de configurer les tables.

Iptables est la boîte à tout faire de Netfilter. Cette commande va pouvoir :

- Rajouter des règles / chaînes.
- Supprimer des règles / chaînes.
- Modifier des règles / chaînes.
- Afficher les règles / chaînes

Comme toute commande Linux qui se respecte, "iptables" est un programme qui se lance en ligne de commande, et qui attend de nombreux paramètres. Voici quelques options nécessaires pour l'utilisation d'Iptables

Option	paramètre	Paramètre optionnel	Explication	exemple
-t (table)	"filter", "nat", "mangle"	OUI	Indique sur quelle table nous voulons travailler. Si aucun paramètre n'est fourni, c'est la table filter qui est sélectionnée par défaut.	"iptables -t nat ..." permet de travailler sur ta table "NAT".
-F(Flush)	"filter", "nat", "mangle"	OUI	Supprime toutes les règles d'une chaîne prédéfinie (tel "PREROUTING", "INPUT","FORWARD", "OUTPUT" et "POSTROUTING"). Si aucun paramètre n'est donné, toutes les chaînes	"iptables -F" supprime toutes les chaînes prédéfinies de la table "filter".

			prédéfinies sont supprimés.	
-X (eXclude)	Chaine utilisateur	OUI	Supprime une chaîne utilisateur. S'il n'y a aucun paramètre, toutes les chaînes utilisateurs sont supprimées.	"iptables -X perso_3" supprime la chaîne utilisateur "perso_3".

Tableau 5.03 : *résumant les options de Netfilter*

5.6.2.1.3 *Exemple complet du firewall*

La règle de filtrage universellement reconnue :

Premièrement, vider toutes les chaînes de toutes les tables de Netfilter, afin de savoir exactement ce que l'on a dans notre firewall. Mais il ne faudra pas rester trop longtemps dans cette situation, car la machine sera sans aucune protection. [22]

Deuxièmement, interdire par défaut tous les paquets. Pour cela, nous allons utiliser l'option "-P" ("Politique par défaut) des chaînes INPUT, FORWARD et OUTPUT de la table filter.

Dans un dernier temps, nous n'allons autoriser que certains flux bien particuliers.

Concernant l'ordre des règles : Lorsque nous appelons la commande "iptables" pour rajouter/supprimer des règles, l'ordre d'insertion de celles-ci à une certaine importance. Si une première règle supprime un certain type de paquets, une seconde règle écrite un peu plus loin dans le script ne verra jamais ces paquets. Donc inutile de les accepter, ou de les supprimer de nouveau. Mais en général, comme on écrit uniquement des règles pour accepter des paquets, il n'y pas d'importance dans l'ordre des règles.

Donc sur la machine Phoenix

En tapant iptables -L pour lister des règles pour la chaine affichée

Remise à zéro des règles de filtrage, il faut supprimer les tables pré-définies (option " -F") et toutes les tables utilisateurs (option "-X").Que nous en ayons déjà ou pas écrite n'a aucune importance, on supprime tout

```
[root@phoenix /]# iptables -t filter -F
[root@phoenix /]# iptables -t filter –X
```

Définition de la politique (cibles) par défaut : La table filter possède 3 chaînes, donc elles sont toutes les trois à initialiser. Par défaut, on décide donc de tout détruire (DROP) :

```
[root@phoenix /]# iptables -t filter -P INPUT DROP
```

[root@phoenix /]# iptables -t filter -P OUTPUT DROP
[root@phoenix /]# iptables -t filter -P FORWARD DROP

A ce stade là, on a court-circuité tout le système de réseau. Toutes les connexions réseaux sont hors service. Pas un logiciel que vous utilisez ne peut accéder au réseau, si on test les connexions avec ping on aura une réponse comme suit.

[root@phoenix /]$ ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted

--- localhost.sky.net ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2011ms

Autorisons maintenant quelques connexions : Dans notre réseau, nous avons deux cartes réseaux ("eth0" et "eth1"), ainsi que l'interface de loopback ("lo").Occupons nous donc de chacune des 3 interfaces :lo (réseau virtuel localhost) : Nous pouvons avoir toute confiance en ce réseau, car il est interne à la mémoire de notre machine. Nous allons donc autoriser ("-j ACCEPT") toutes les connexions sortantes des processus locaux ("-A OUTPUT") par cette interface virtuelle ("-o lo") ayant une adresse de loopback ("-s 127.0.0.0/8"), et à destination des machines de ce réseau virtuel (-d "127.0.0.0/8) :

[root@phoenix /]# iptables -t filter -A OUTPUT -o lo -s 127.0.0.0/8 -d 127.0.0.0/8 -j ACCEPT

Puis nous allons faire l'inverse, c'est à dire autoriser ("-j ACCEPT") toutes les connexions rentrantes dans les processus locaux ("-A INPUT"), par cette interface virtuelle ("-i lo"), venant des machines de ce réseau virtuel (-s "127.0.0.0/8) et à destination des adresses de loopback ("-d 127.0.0.0/8")

[root@phoenix /]# iptables -t filter -A INPUT -i l o -s 127.0.0.0/8 -d 127.0.0.0/8 -j ACCEPT

Et nous pouvons immédiatement vérifier que le "ping localhost" fonctionne à nouveau :

[root@phoenix /]$ ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost.sky.net (127.0.0.1): icmp_seq=1 ttl=64 time=0.134 ms
64 bytes from localhost.sky.net (127.0.0.1): icmp_seq=2 ttl=64 time=0.091 ms
--- localhost ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.091/0.112/0.134/0.023 ms

Autorisons les connexions pour l'interface eth0

[root@phoenix /]# iptables -t filter -A OUTPUT -o eth0 -s 192.168.10.0/24 -d 192.168.10.0/24 -j ACCEPT
[root@phoenix /]# iptables -t filter -A INPUT -i eth0 -s 192.168.10.0/24 -d 192.168.10.0/24 -j ACCEPT

Si on tests la connexion vers la machine monentreprise, on a

[root@phoenix /]$ ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
64 bytes from monentreprise (192.168.10.2): icmp_seq=1 ttl=64 time=0.134 ms
64 bytes from monentreprise (192.168.10.2): icmp_seq=2 ttl=64 time=0.091 ms
--- localhost ping statistics ---
2 packets transmitted, 2 received, 0% packet loss,

Pour la carte réseau eth1, il y a quelques problèmes car on ne connait pas toutes les adresses IP qui se connectent sur l'Internet

Pour cela on va autoriser les connexions vers les services web qui nous intéresse, à savoir le HTTP (port 80 en TCP), et le HTTPS (443 en TCP), et cela pour toutes les machines. Seules les requêtes en direction et venant des ports seront autorisées :

[root@phoenix /]# iptables -t filter -A OUTPUT -o eth1 -s 10.0.0.0/8 -p tcp --dport 80 -j ACCEPT
[root@phoenix /]# iptables -t filter -A OUTPUT -o eth1 -s 10.0.0.0/8 -p tcp --dport 443 -j ACCEPT
[root@phoenix /]# iptables -t filter -A INPUT -i eth1 -d 10.0.0.0/8 -p tcp --sport 80 -j ACCEPT
[root@phoenix /]# iptables -t filter -A INPUT -i eth1 -d 10.0.0.0/8 -p tcp --sport 443 -j ACCEPT

Le problème c'est qu'une machine ne peut pas accéder à leurs propres ressources car elle ne passe pas par une interface physique mais par une interface de loopback, si on teste la connexion, l'opération ping n'est pas permise.

```
[root@phoenix /]$ ping phoenix
PING phoenix (192.168.10.1) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
```

Pour en remédier, on va supprimer les règles précédentes

```
[root@phoenix /]# iptables  -t filter  -D  OUTPUT 1
 [root@phoenix /]# iptables  -t filter  -D  INPUT 1
[root@phoenix /]# iptables  -t filter  -A  OUTPUT  -o  lo -s  0.0.0.0/0  -d 0.0.0.0/0  -j ACCEPT
[root@phoenix /]# iptables  -t filter  -A  INPUT  -i  lo  -s  0.0.0.0/0  -d 0.0.0.0/0  -j ACCEPT
```

Maintenant on peut accéder à ses propres ressources, si on teste la connexion la commande ping devra marcher

Si on utilise le second script, le pirate ne peut plus accéder à monentreprise de plus il voit la machine Phoenix comme étant arrêtée.

Un pirate est souvent quelqu'un qui est fort en informatique, notamment il sait lire le man de nmap et connait l'option –g

```
[root@pirate /]# nmap phoenix1  -g 80
Starting nmap V. 3.0
Interesting ports on phoenix1(10.0.0.1):
(The 1585 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp      open ftp
23/tcp      open telnet
25/tcp      open smtp
53/tcp      open domain
80/tcp      open http
110/tcp     open pop-3
111/tcp     open sunrpc
139/tcp     open netbios-ssn
```

307/tcp filtered unknown

404/tcp filtered nced

443/tcp open https

511/tcp filtered passgo

578/tcp filtered ipdd

607/tcp filtered nqs

3306/tcp open mysql

Donc le pirate connait les ports qui sont ouverts et peut accède facilement au système.

Pour le renvoyer on va utiliser le suivi de connexion de Netfilter ou conntrack

- **Conntrack**

Cette technique est vraiment une avancée en matière de firewall. Netfilter se base sur la poignée de main ("handshake), afin de déterminer si une connexion a été initialisée par Phoenix ou non. Pour toute nouvelle connexion sortante, il associe l'état "NEW" ("nouveau" en anglais) à la connexion, et stocke cette information en mémoire. Quand il verra arriver d'autres connexions venant de l'extérieur en réponse à cette connexion "NEW", il leur attribuera alors l'état " ESTABLISHED" ("établie" en anglais). Ainsi, pour une connexion rentrante et qui ne se trouve pas déjà dans la mémoire de Netfilter, celui-ci pourra en déduire qu'elle a été initialisée par l'extérieur, et lui attribuera l'état " INVALID". Dans ce cas, et si il a été configuré pour, Netfilter pourra refuser ("DROP") ou rejeter ("REJECT") cette connexion. [22]

La figure suivante permet d'illustrer cette technique

Figure 5.12 : *Suivi de connexion*

Pour mettre en œuvre cette technique. Le système de suivi de connexion de Netfilter n'est pas forcément compilé dans le kernel, donc si ce n'est pas le cas, on doit d'abord charger le module ip_conntrack

[root@phoenix /]# modprobe ip_conntrack

Si on envisage d'utiliser les clients FTP en mode passif, ou qu'on compte d'utiliser l'IRC, on a la possibilité de charger les modules "ip_conntrack" qui supportent ces protocoles :

[root@phoenix /]# modprobe ip_conntrack_ftp

[root@phoenix /]# modprobe ip_conntrack_irc

Maintenant, comment indiquer à Netfilter que nous ne désirons laisser passer que les connexions sortantes initialisées par la machine, mais aussi de ne laisser passer que celles qui sont en réponse avec les premières

[root@phoenix /]# iptables -A OUTPUT -o eth1 -s 10.0.0.1 -d 0.0.0.0/0 -p all -m state --state ! INVALID -j ACCEPT

[root@phoenix /]# iptables -A INPUT -i eth1 -s 0.0.0.0/0 -d 10.0.0.1 -p all -m state --state RELATED,ESTABLISHED -j ACCEPT

Le paramètre "-m state" signifie qu'on a besoin du module "state" (celui du suivi de connexion), et de ses options particulières."--state" indique les états qui vont être utilisés pour nos règles. "! INVALID" : comme vu plus haut, le module de suivi de connexion gère 4 états, NEW, ESTABLISHED, RELATED et INVALID. Ce paramètre indique que l'on accepte uniquement les connexions qui ne sont pas invalides, donc qui sont "NEW, ESTABLISHED, RELATED". Ceci est uniquement une manière plus rapide d'écrire qu'il faut que les connexions soient d'un des trois états "NEW, ESTABLISHED, RELATED".

A ce stade le pirate ne peut plus accéder au système

[root@pirate /]# nmap phoenix1.internet.net -g 80 -P0

Starting nmap V. 3.00

All 1601 scanned ports on phoenix1.internet.net (10.0.0.1) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 1721 seconds

- **IP masquerading**

Jusqu'à présent, la machine monentreprise de notre réseau n'a pas été très utilisée. Son activité réseau est restreinte à celle du réseau de l'entreprise. Alors que Phoenix, lui, peut se

connecter au réseau interne. Dans cette étude, notre but c'est de transformer Phoenix en une passerelle entre les réseaux de l'entreprise nommé entreprise.mg et internet. [22]
Pour réaliser ceci, il nous faut réaliser plusieurs opérations :

- La première, c'est de charger les modules dont on va avoir besoin. En premier, on a besoin du module de NAT, c'est-à-dire "iptables_nat". Comme on veut aussi faire du suivi de connexion sur les paquets NAT, on chargera de même les modules NAT FTP et IRC, "ip_nat_ftp" et "ip_nat_irc" :

[root@phoenix /]# modprobe iptable_nat
[root@phoenix /]# modprobe ip_nat_ftp
[root@phoenix /]# modprobe ip_nat_irc

- On va initialiser la table NAT

[root@phoenix /]# iptables -t nat -F
[root@phoenix /]# iptables -t nat –X

- Pour ce qui est des cibles par défaut des chaînes de la table NAT, on accepte toutes les connexions. Il n'est pas nécessaire de faire pointer ces cibles sur "DROP", car la sécurité est établie au niveau de la table "Filter", par le "DROP" par défaut de la chaîne FORWARD :

[root@phoenix /]# iptables -t filter -P FORWARD DROP
[root@phoenix /]# iptables -t nat -P PREROUTING ACCEPT
[root@phoenix /]# iptables -t nat -P POSTROUTING ACCEPT
[root@phoenix /]# iptables -t nat -P OUTPUT ACCEPT

- Maintenant on va faire suivre sur le réseau internet, les connexions issues du réseau de l'entreprise. On ne fera suivre que les connexions qui sont à destination du réseau internet, et non celles destinées à la machine Phoenix elle-même. Pour cela, on a besoin d'utiliser la table "Filter», afin de faire suivre les paquets venant de la carte eth0 à la carte eth1, et vice versa. En plus de cela, comme ce sont uniquement les connexions initialisées par le réseau interne qu'on désirons faire sortir, on rajoutera un peu de suivi de connexion.

[root@phoenix]# iptables -t filter -A FORWARD -i eth0 -o eth1 -s 192.168.10.0/24 -d 0.0.0.0/0 \ -m state --state ! INVALID -j ACCEPT

[root@phoenix]# iptables -t filter -A FORWARD -i eth1 -o eth0 -s 0.0.0.0/0 -d 192.168.10.0/24 \ -m state --state ESTABLISHED,RELATED -j ACCEPT

L'accumulation des paramètres "-i", "-o", "-s", "-d" et "--state" permettent de garantir que seul les connexions initialisées par le domaine du réseau d'entreprise seront autorisées à passer, et non l'inverse. [22]

Pour le moment, les paquets venant du réseau de notre entreprise et sortant par l'interface eth1, ont :

- pour adresse de destination, une adresse du réseau internet.net, ce qui est parfaitement normale. Celle de web.internet par exemple
- pour adresse source, l'adresse d'une machine du domaine de notre entreprise qui est entreprise.mg, comme par exemple celle du machine monentreprise, mais ce domaine est un réseau privé, dont l'adresse IP n'est pas du tout routable sur Internet. Conclusion : lorsque web.internet. recevra la requête, il ne saura absolument pas où envoyer la réponse. Il va donc falloir que Phoenix subtilise l'adresse IP source des trames qui le traverse, et la remplace par la sienne. C'est là qu'intervient la table NAT, avec la cible "MASQUERADE" (pour "masquage" en anglais) :

[root@phoenix /]# iptables -t nat -A POSTROUTING -o eth1 \ -s 192.168.10.0/24 -j MASQUERADE

- Enfin, maintenant que tout le NAT est configuré, il ne reste plus qu'à autoriser dûment du Linux à faire jouer son rôle de gateway. Pour cela, il faut simplement écrire un "1" dans le "/proc/sys/net/ipv4/ip_forward". Ce fichier est en fait un fichier virtuel, qui permet de dialoguer directement avec le kernel. Nous allons donc utiliser la commande suivante :

  [root@phoenix /]# echo 1 > /proc/sys/net/ipv4/ip_forward
- Le NAT étant maintenant configuré et activé, il reste à configurer les machines du réseau de l'entreprise, afin de leur indiquer quelle est la passerelle. C'est chose faite en lançant par exemple sur la machine monentreprise :

[root@monentreprise /]# route add default gw phoenix.entreprise

- **Port forwarding**

- Tout d'abord, on doit initialiser la table NAT, tout comme nous l'avons fait pour l'IP masquerading. Et aussi charger le module "iptables_nat" :

[root@phoenix /]# modprobe iptable_nat

[root@phoenix /]# iptables -t nat -F

[root@phoenix /]# iptables -t nat -X

[root@phoenix /]# iptables -t filter -P FORWARD DROP

[root@phoenix /]# iptables -t nat -P PREROUTING ACCEPT

[root@phoenix /]# iptables -t nat -P POSTROUTING ACCEPT

[root@phoenix /]# iptables -t nat -P OUTPUT ACCEPT

- On va partager un serveur http. On utilise le "suivi de connexion", afin de ne pas accepter les paquets ICMP volontairement mal formatés :

[root@phoenix /]# iptables -t filter -A INPUT -i eth1 -s 0.0.0.0/0 -d 10.0.0.1 \-p icmp -m state --state ! INVALID -j ACCEPT

[root@phoenix /]# iptables -t filter -A OUTPUT -o eth1 -s 10.0.0.1 -d 0.0.0.0/0 \-p icmp -m state --state RELATED,ESTABLISHED -j ACCEPT

- On va maintenant faire suivre un certain type de paquets de l'interface "eth1" à l'interface "eth0" : Ce sera les paquets à destination du serveur HTTP. De même qu'on laissera passer les paquets en réponse. Là encore, nous utilisons du "conntrack" afin d'améliorer la sécurité de ce suivi de port :

[root@phoenix /]# iptables -t filter -A FORWARD -i eth1 -o eth0 -s 0.0.0.0/0 \

-d 192.168.10.2 -p tcp --dport 80 \-m state --state ! INVALID -j ACCEPT

[root@phoenix /]# iptables -t filter -A FORWARD -i eth0 -o eth1 -s 192.168.10.2 \

-d 0.0.0.0/0 -p tcp --sport 80 \-m state --state RELATED,ESTABLISHED -j ACCEPT

- Pour les paquets entrant sur phoenix1.net et à destination du port 80, on va modifier l'adresse de destination. Ce ne sera plus phoenix1.net, mais monentreprise.entreprise.mg c'est à dire notre réel serveur HTTP. Pour cela, on va utiliser dans la table NAT, la chaîne "PREROUTING" et la cible "DNAT

[root@phoenix /]# iptables -t nat -A PREROUTING -i eth1 -s 0.0.0.0/0 \-d 10.0.0.1 -p tcp --dport 80 \-m state --state ! INVALID -j DNAT --to-destination 192.168.10.2:80

- La seconde spécificité du "port forwarding", c'est de modifier aussi l'adresse source de la requête. En effet, si on laisse l'adresse source actuelle (une adresse de 10.0.0.0/8 par exemple), monentreprise.entreprise.mg sera bien ennuyé pour répondre, car ce sera une adresse d'un réseau qu'il ne peut pas joindre. Évidement, nous pourrions indiquer à monentreprise.entreprise.mg que phoenix0.net (celui qui relie le réseau privé avec Phoenix) est une passerelle, et dans ce cas là les paquets retrouveraient tout de suite la sortie du réseau entreprise.mg. Mais, et même si cette solution marche effectivement très bien, c'est une solution particulièrement mal propre, Donc, modifions cette adresse source :

[root@phoenix /]# iptables -t nat -A POSTROUTING -o eth0 -s 0.0.0.0/0 \
-d 192.168.10.2 -p tcp --dport 80 \-m state --state ! INVALID -j SNAT --to-source 192.168.10.1

au niveau de Netfilter, tout est configuré. Il ne reste qu'à activer le NAT par la commande suivant

[root@phoenix /]# echo 1 > /proc/sys/net/ipv4/ip_forward

- **LOG**

C'est la méthode la plus standard pour logger des trames. Il s'agit simplement de créer une règle "iptables" dont la cible ("-j [cible]") n'est pas "ACCEPT" ou "DROP", mais tout simplement "LOG". [22]

[root@phoenix /]# iptables -t filter -A INPUT -j LOG

Une autre méthode est de définir un "niveau de log" ("log level" en anglais), qui rajoute une autre information aux logs, ce qui permet au demon de log (un programme appelé "syslogd") de stocker ces logs dans un autre fichier.

[root@phoenix /]# iptables -t filter -A INPUT -j LOG --log-level=4
[root@phoenix /]# less /usr/include/sys/syslog.h
#define LOG_WARNING 4 /* warning conditions */
[root@phoenix /]# less /etc/syslog.conf
kern.=warn -/var/log/kernel/warnings

- **ULOG**

ULOG est module du Kernel qui a été spécialement conçu pour recevoir les logs de Netfilter. [22]. Il y a certaines contraintes à son utilisation :

- Kernel récent : il faut un Kernel >= 2.4.18-pre8 pour pouvoir l'utiliser

- Option de compilation : il faut que le kernel soit compilé avec l'option CONFIG_IP_NF_TARGET_ULOG=m.
- Une fois compilé, le module ipt_ULOG.o doit se trouver sur le disque dur (/lib/modules/[version du kernel]/kernel/net/ipv4/netfilter/ipt_ULOG.o.gz par exemple) :

[root@phoenix /]# find /lib/modules/‘uname -r‘/ -iname "*ULOG*" /lib/modules/2.4.21-0.13mdksmp/kernel/net/ipv4/netfilter/ipt_ULOG.o.gz

- On doit récupérer et installer le demon "ulogd" sur la machine
- Il faut configurer le demon ulogd. Pour cela, il faut éditer son fichier de configuration.
- Le demon ULOG ("ulogd") doit tourner sur la machine. L'idéal est de le lancer au démarrage, en même temps que les autres demons de la machine.
- Pour démarrer le demon de Ulog
  [root@phoenix /]# /etc/rc.d/rc5.d/S10ulogd start
- Pour verifier que le demon fonctionne correctement
  [root@phoenix /]# cat /var/log/ulogd.log
- Configurez Netfilter pour qu'il utilise la cible ULOG au lieu de la cible LOG. Ici, on log tout ce qui va être supprimé par la chaîne "INPUT" :
  [root@phoenix /]# iptables -t filter -A INPUT -p all -j ULOG --ulog-prefix=DefaultDrop

5.6.3 Réalisation du firewall à l'aide d'un squid

Squid est un logiciel proxy pour les protocoles http, Gopher et FTP. Il permet de construire facilement un pare feu de type multi-domicilé. En dehors de son utilisation à des fins de sécurité, il peut être utilisé comme cache pour améliorer les performances d'accès web. [23]

Pour cette réalisation, supposons qu'on ait deux réseaux reliés par notre pare feu

- Le réseau extérieur est le réseau 10.0.0.0 et l'on atteint par l'interface eth1 d'adresse 10.0.0.1
- Le réseau intérieur est le réseau 192.168.10.0 et il est relié par l'interface eth0 d'adresse 192.168.10.6
- Et une machine qu'on va transformer en firewall, et c'est sur cette machine qu'on va installer le squid

- Paquet à installer

aptitude install squid

- Configuration du squid

Le fichier de configuration du squid se trouve dans /etc/squid/squid.conf

Le fichier de configuration de Squid comporte de nombreuses pages (surtout des commentaires), mais il y a très peu de choses à changer pour le faire fonctionner

- On va enregistrer un nouveau fichier de configuration et appelons ce fichier par squid.conf.sav

#cd /etc/squid/
cp squid.conf squid.conf.sav

Dans le fichier de configuration, on va rechercher la partie concernant la déclaration des acl et on va ajouter une ligne concernant la configuration du réseau, et comme le nom de notre domaine est entreprise.mg, on va ajouter ce nom dans la fichier de configuration

acl entreprise.mg src 192.168.10.0/255.255.255.0

Ensuite, quelques lignes plus bas avant la dernière ligne « http_access deny all »on va ajouter la ligne suivante :

http_access allow entreprise.mg

on va redémarrer le serveur pour prendre en compte les modifications :

/etc/init.d/squid restart

- Configuration du poste client

Dans la partie configuration du proxy, il faut indiquer le nom ou l'adresse IP du proxy et le port par défaut 3128.

- Il est possible de désactiver le cache du navigateur en le mettant à 0 car celui du proxy est suffisant.
- Il est possible aussi d'indiquer une liste de serveurs accessibles sans passer par le proxy (ex : Intranet)

- Vérification du fonctionnement

La commande suivante permet de surveiller les logs du proxy pour vérifier que tout fonctionne correctement :

tail - f /var/log/squid/access.log

- installation du squidguard

SquidGuard est un filtre, un redirecteur et un plugin de contrôle d'accès pour Squid.

Pendant cette réalisation on va prendre un blacklist (liste des sites sensibles) contenant les nom du site qu'on va interdire leur entrée dans notre réseau local. Pour cela

- Paquet à installer:

aptitude install squidguard

Maintenant on va récupérer la liste du site sensible

tar zxvf blacklist.tar.gz -C /var/lib/squidGuard/db/

cd /var/lib/squidGuard/db

mv blacklist/* .

rm -rf blacklist

Le fichier de configuration de SquidGuard est /etc/squid/squidGuard.conf. [24]
Pour la configuration, on va prendre notre réseau précedent, donc on a

- Adresses de type : 192.168.10.x
- Adresse du serveur proxy : 192.168.10.1
- Nom du serveur proxy : serveur
- Port d'écoute de Squid : 3128.
- Stations autorisées à utiliser Internet : 192.168.10.50 et de 192.168.10.100 à 192.168.10.125

- configuration

/etc/squid/squidGuard.conf

```
dbhome /var/lib/squidGuard/db
logdir /var/log/squid

# Definition des sources :

src admin {
ip 192.168.10.1
}

src poste {
ip 192.168.10.50
}

src multipostes {
ip 192.168.10.100-192.168.10.125
}

# Definition de la base de données de filtrage utilisée
dest adult {
domainlist adult/domains
urllist adult/urls
}
dest publicite {
domainlist publicite/domains
urllist publicite/urls
}
dest warez {
domainlist warez/domains
urllist warez/urls
}
dest porn {
domainlist porn/domains
urllist porn/urls
}
```

```
# Definition des ACL

acl {
admin {
pass all
}

poste {
pass !porn !adult !publicite !warez all
redirect http://mon_serveur/interdiction.html
}

multipostes {
pass !porn !adult !publicite !warez all
redirect http://mon_serveur/interdiction.html
}

default {
pass none
redirect http://mon_serveur/interdiction.html
}
}

# pour admin tout est autorisé, pour poste et multipostes tout est autorisé sauf porn adult publicite et warez
# "redirect http://mon_serveur/interdiction.html" correspond à la redirection du client en cas d'accès refusé.

# FIN /etc/squid/squidGuard.conf #
```

SquidGuard comme Squid doit être lancé par un utilisateur différent de root, par mesure de sécurité. Pour cela, en tant que root, on va créer les groupe et utilisateur "proxy" s'ils n'existent pas, par

groupadd proxy

useradd -g proxy -d /etc/squid -s /bin/bash proxy

passwd proxy

Il ne reste plus qu'à attribuer les bonnes permissions aux répertoires

chown -R proxy.proxy /var/lib/squidGuard /etc/squid /usr/bin/squidGuard /usr/bin/squid /var/log/squid /var/spool/squid

On va créer la base de données de filtrage par :

squidGuard -C all

On va éditez le fichier /etc/squid/squid.conf et décommentez la ligne :

redirect_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf

Maintenant il faut redémarrer le serveur pour prendre en compte les modifications

- Résultat :

La politique du site :

- laisser entrer le moteur de recherche GOOGLE pour que les personnels peuvent rechercher des documents
- interdire les sites pornographiques. Si un personnel ouvre le moteur de recherche google, alors il aura comme réponse la figure suivante

Figure 5.13 : *site à laisser passer*

Par contre, s'il ouvre un site adulte, il aura comme réponse la figure ci-dessous

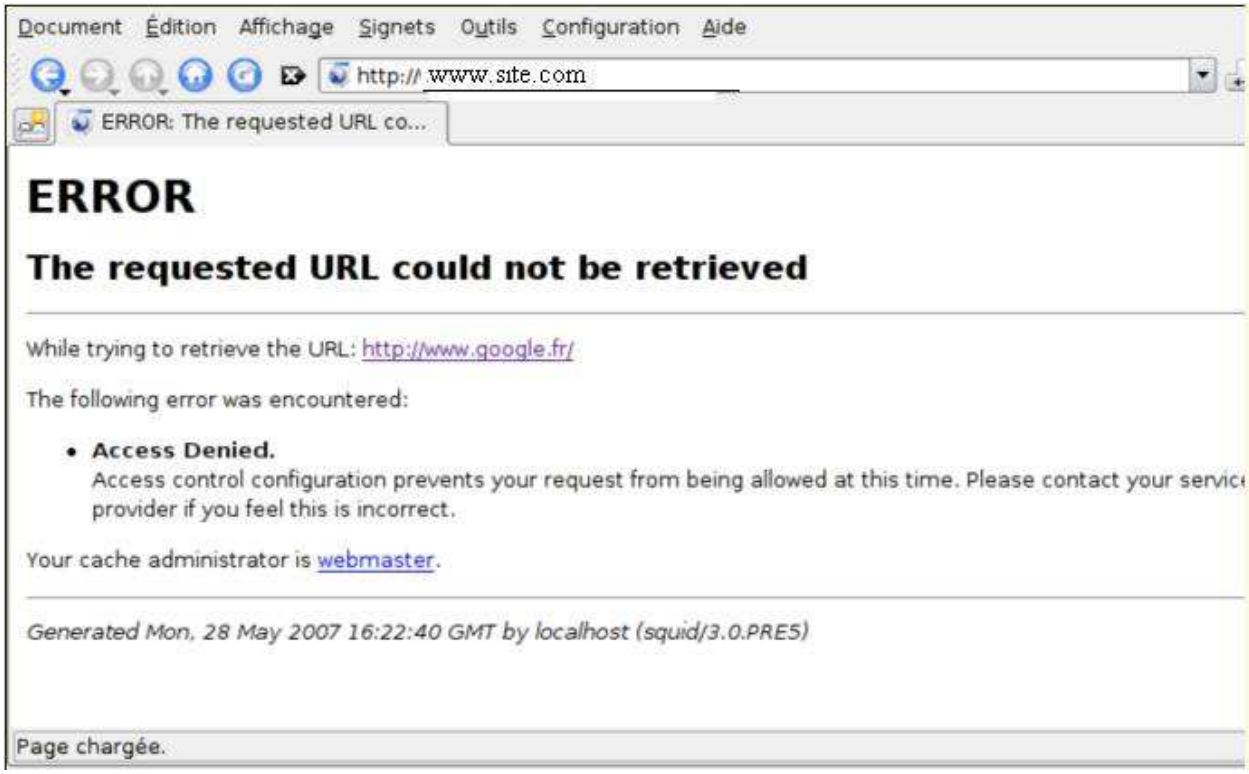

Figure 5.14 : *site filtré*

CONCLUSION

On peut en déduire de ce travail qu'un Intranet est un réseau LAN basé sur le concept de couche fonctionnelle du modèle OSI en utilisant les services offerts par Internet. Intranet est un des moyens pour améliorer la circulation des informations dans une entreprise, et facilite plusieurs taches parce qu'il offre plusieurs services comme le transfert de fichier, l'utilisation du navigateur web pour accéder à des documents, l'utilisation du nom du domaine pour accéder aux différentes hôtes dans l'entreprise, on peut aussi faire des discussions en ligne en faisant un forum ou directement appelé d'autre personnel via un serveur vocal.

Pendant ce travail, on a utilisé le système d'exploitation linux, car Linux est le système qui connaît actuellement le plus grand développement sur l'Internet ou Intranet. Principalement pour les raisons diverses comme l'utilisation de trois logiciels serveurs leaders sur l'Internet : Apache en serveur Web, Postfix ou sendmail en serveur courrier et Bind en serveur DNS ; moins d'interruptions de service grâce à une gestion intelligente de l'installation des logiciels, etc.

De plus, actuellement on ne peut plus reculer devant l'expansion de l'internet, mais on ne peut non plus exposer nos réseaux locaux, à des innombrables attaques venant de lui.
Parmi tant d'autres sécurités, nous venons de découvrir le firewall, qui est un de sécurité le plus puissant pour stopper les intrus et les malfaiteurs de l'internet. Il se base sur le filtrage de paquets, et on utilise le service mandataire pour le faire fonctionner. Il sert les numéros de ports ou les adresses réseau pour bloquer ou laisser passer les services internet ou ceux qui viennent du réseau protégé. L'implémentation et la réalisation du firewall nécessite un politique venant du site à protéger.
Cependant, firewall ne peut pas garantir la sécurité totale d'un réseau local, néanmoins il est un des outils les plus puissants en termes de sécurisation avec la collaboration des personnels qui utilisent le réseau.
Nous espérons que ce dossier vous aura permis d'acquérir de bonnes connaissances en termes de création et d'utilisation d'un intranet et surtout la sécurisation d' un réseau local via d'un firewall.

ANNEXE 1

Le système de fichier sous linux :

/ : Répertoire "racine", point d'entrée du système de fichiers

/boot : Répertoire contenant le noyau Linux

/bin : Répertoire contenant les exécutables de base, comme par exemple cp, mv, ls, etc...

/dev : Répertoire contenant des fichiers spéciaux nommés *devices* qui permettent le lien avec les périphériques de la machine

/etc : Répertoire contenant tous les fichiers de configuration du système

/home : Répertoire contenant les fichiers personnels des utilisateurs

/lib : Répertoire contenant les librairies et les modules du noyau (/lib/modules)

/lost+found : Répertoire spécial contenant les fichiers abimés ou trouvés après un crash du disque dur. Il y en a un dans la racine de chaque partition Linux.

/media : Répertoire vide dans lequel on "montera" (cf ci-dessous) les médias externes (CD, disquette, clé USB).

/mnt : Répertoire vide dans lequel on "montera" (cf ci-dessous) d'autres systèmes de fichiers

/proc Répertoire contenant des fichiers spéciaux représentant certaines caractéristiques matérielles ou Certains paramètres du noyau.

/root : Répertoire personnel de l'administrateur.

/sbin : Répertoire contenant les exécutables destinés à l'administration du système.

/sys : Répertoire contenant des fichiers spéciaux représentant certaines caractéristiques matérielles ou certains paramètres du noyau.

/tmp : Répertoire contenant des fichiers temporaires utilisés par certains programmes

/usr Répertoire contenant les exécutables des programmes (/usr/bin et /usr/sbin), la documentation

(/usr/doc), et les programmes pour le serveur graphique (/usr/X11R6).

/var : Répertoire contenant les fichiers qui servent à la maintenance du système.

ANNEXE 2

Les options Iptables

Option	Paramètre	Paramètre optionnel	Explication	Exemple
-P (policy)		Non	Définie la politique (ou cible) par défaut d'une chaîne. Seules les chaînes prédéfinies peuvent avoir un comportement par défaut. Cette cible ne sera appliquée qu'après l'exécution de la dernière règle de la chaîne.	"iptables -P INPUT DROP" supprime par défaut tout les trames dans la chaîne "INPUT". Si aucune règle plus "souple" n'est définie, aucun paquet réseau n'arrivera aux processus utilisateurs de notre machine. C'est efficace comme technique, mais peu fonctionnel.
-N (new)		Non	Cette option crée une nouvelle chaîne utilisateur. Par la suite, des règles doivent êtres créées, afin de remplir cette chaîne. Sinon, elle ne sera pas très utile !	"iptables -N LogAndDrop" crée une chaîne utilisateur dont le nom laisse supposer que l'on va logger les paquets, puis les supprimer.
-A (append)		Non	Ajoute une règle à une chaîne prédéfinie ou utilisateur. Nous allons utiliser majoritairement cette commande.	"iptables -A INPUT ..." ajoute une règle à la table des paquets entrant dans l'espace des programmes.
-D (delete)		Non	Supprime une règle dans une chaîne particulière. Le numéro de la règle peut être retrouvé avec la commande "iptables -L" ou "iptables -L -n"	"iptables -D OUTPUT 1 -t mangle" supprime la 1ère règle de la chaîne "OUTPUT" de la table "Mangle".

-L (list)		Oui	Affiche la liste des règles pour la chaîne indiquée. Ou, si aucune chaîne n'est indiquée, cela affichera les règles pour toutes les chaînes de la table indiquée. Note : Rajouter à "-L" les options "-n" et "-v" est très utile.	"iptables -L -n -v" affiche le maximum d'informations sur les règles de la table "filter".
-j (jump)		Non	Défini l'action à prendre si un paquet répond aux critères de cette règle. Les principales valeurs sont : ACCEPT, DROP, REJECT, LOG	"iptables -A OUPUT -j DROP" supprime tous les paquets sortant des processus locaux. Ca, c'est de la censure
-i (input)		Non	Critère sur l'interface réseau dont provient-le paquet	"iptables -A INPUT -i eth0 ..." filtre les paquets arrivant aux programmes et venant de l'interface réseau eth0
-o (output)		Non	Critère sur l'interface réseau d'où les paquets vont sortir	"iptables -A OUTPUT -o ppp0" filtre les paquets créés par les programmes et sortant sur Internet.
--state	[!] "NEW", "ESTABLISHED", "RELATED", "INVALID"	Non	Cette option ne s'utilise que cumulée avec l'option "-m state", afin d'être utilisé pour le suivi de connexion	"iptables ... --state NEW,ESTABLISHED ..." filtre les paquets de nouvelles connexions, ou de connexions déjà établies via une " poignée de main ".

Tableau A2.01 : *Options d'Iptables*

BIBLIOGRAPHIE

[1] E.L. Randriarijaona, « *Administration Réseaux*», Cours I5 – TCO, Dép. TCO.- E.S.P.A., A.U. : 2008-2009.

[2] A. Ratsimbazafy, « *réseaux* », Cours I3 – TCO, Dép. TCO.- E.S.P.A., A.U. : 2006-2007.

[3] L. L. Peterson, B. S., « *computer Networks*», Morgan Kaufman, 2000.

[4] http:// www.cisco.com/ccna discovery/

[5] D.Brent Chapman & E.D Zwicky, *« Firewalls»*, O'REILLY, Paris 1996

[6] S. Syan, *« TCP IP »*, Karanjit 1998

[7] http:// www.commentçamarche.com/ architectures client-serveur/

[8] Graig Hunt, *«TCP IP Network Administration »*, O'REILLY

[9] Guy Pujolle, *«Les Réseaux »*, Edition 2003

[10] Elisabeth D. Zwicky, *«Building Firewalls Internet», O'REILLY, Paris 1993*

[11] E.L. Randriarijaona, *«Développement d'entreprise »*, Cours I5 – TCO, Dép. TCO.- E.S.P.A., A.U. : 2008-2009.

[12] http://wikipedia.com/

[13] A. De Lattre, Rémy Carrigue, *« Formation Debian GNU Linux »*, copyright 2005

[14] P. Druout & H. Kamel, *« Configuration, mise en œuvre et administration de serveurs Internet et Intranet sous Linux »*, Africa computing DDTEFP n°93 13 10226 13.

[15] http://www.adnavigo.com/linux/firewall

[16] M. Decorre, *« Linux commandes, outils »*, copyright 1999

[17] Portland, *ARP - Address Resolution Protocol TCP/IP class*, http://www.info-du-net.com .

[18] O. Aubert, *« Le modèle client-serveur »*, *http://*www.networksorcery.com

[19] S. Garfinkel, *« Pratical Unix Security »*, http://www.amazon.com

[20] Sedera Joel, *«Firewall Internet»*, Mémoire de Fin d'études, Dép. Tél. –ESPA., AU. : 2002-

2003.

[21] O. Allard Jacquin, *« Firewall »*, version 0.5.3 copyright 2003

[22] http://www.gnu.org/licenses/gpl.html

[23] http ;// www.sleepycat.com/configuration squid

[24] http://www.coagul.com/firewall

RESUME

La mise à disposition d'un intranet est nécessaire dans une entreprise car il facilite beaucoup l'accès aux divers services de l'entreprise. Sa mis en place nécessite la connaissance approfondie sur le réseau, les différentes configurations de chaque machine cliente et de serveur et les différents outils pour relier les machines comme les routeurs ou switch. Pour le faire, on commence par adresser les différentes machines clientes ou serveurs, choisir une plate forme pour installer le serveur, dans notre cas on a choisi linux et la distribution Debian comme plate forme.

De plus, si une entreprise se connecte à internet, il est nécessaire de protéger ses données, ou ses différents services pour qu'un pirate ne risque pas de voler ces données. Pour cela il est aussi nécessaire de mettre en place un firewall qui interdit l'accès du pirate dans le système. Sa mis en place nécessite la politique de protection du site, la connaissance des différentes outils d'analyse et la combinaison des différentes architectures pour renforcer la sécurité du site.

ABSTRACT

Placed at the disposal of an Intranet is necessary in a company because it facilitates much the access to the various services of the company. Its set up requires thorough knowledge on the network, various configurations of each machine client and server and various tools to connect the machines like the routers or switch. To do it, one starts by addressing the various machines client or server, to choose a punt forms to install the server, in our case one chose linux and the Debian distribution like punt forms.

Moreover, if a company is connected to Internet, it is necessary to protect its data or its various services so that a pirate is not likely to steal these data. For that it is also necessary to set up a firewall which prohibits the access of the pirate in the system. Its set up requires the policy of protection of the site, the knowledge of different tools from analysis and the combination of various architectures to reinforce the safety of the site.

Nom: HASINAVALONA

Prénom : Henintsoa Seth Etienne

Adresse de l'auteur : Lot VA 37 FA Bis B Tsiadana

Antananarivo -101

Mail : navalonahenintsoa@yahoo.fr

Contact : 0330791160

Titre de mémoire :

MISE EN PLACE D'UN RESEAU INTRANET SOUS LINUX DANS UNE ENTREPRISE ET MISE A DISPOSITION D'UN FIREWALL INTERNET

Nombre de page : 133

Nombres de figures : 45

Nombre de tableaux : 4

Nombres d'annexes : 2

Mots clés : Réseau, Linux, Internet, Intranet, Firewall, Iptables, Squid, Squidguard, table, List

Directeur de mémoire : Monsieur ANDRIAMIASY Zidora